Zur Sicherheitsnachweisführung einer bordautonomen satellitenbasierten Ortungseinheit für den Schienenverkehr

Von der Fakultät für Maschinenbau

der Technischen Universität Carolo-Wilhelmina zu Braunschweig

zur Erlangung der Würde

eines Doktor-Ingenieurs (Dr.-Ing.)

genehmigte Dissertation

von:	Dipl.-Ing. Hansjörg Manz
aus:	Dresden

eingereicht am:	11.02.2016
mündliche Prüfung am:	04.05.2016

Gutachter:	Prof. Dr.-Ing. Dr. h.c. mult. Eckehard Schnieder
	Prof. Dr.-Ing. Jochen Trinckauf
Vorsitzender:	Prof. Dr.-Ing. Peter Hecker

2016

„Probleme kann man niemals mit derselben Denkweise lösen,
durch die sie entstanden sind.“
Albert Einstein

Vorwort

Die vorliegende Arbeit entstand während meiner Beschäftigung als wissenschaftlicher Mitarbeiter am Institut für Verkehrssicherheit und Automatisierungstechnik der TU Braunschweig in den Jahren 2009-2016. Zu Beginn möchte ich mich bei allen Unterstützern bedanken, die mich während der Fertigstellung begleitet haben.

Dem Institutsleiter im Ruhestand, Herrn Prof. Dr.-Ing. Dr. h.c. mult. Eckehard Schnieder danke ich insbesondere für seine langjährige Unterstützung, für teilweise kontroverse aber jederzeit zielorientierte wissenschaftliche Diskussionen und seine sehr persönliche Begleitung. Des Weiteren danke ich Herrn Prof. Dr.-Ing. Jochen Trinckauf, Leiter der Professur für Verkehrssicherungstechnik der TU Dresden, für sein kritisches Interesse an meiner Arbeit und die Begleitung als Koreferator. Ebenso möchte ich mich bei Herrn Prof. Dr.-Ing. Peter Hecker, Leiter des Instituts für Flugführung der TU Braunschweig, für die Übernahme des Vorsitzes der Prüfungskommission bedanken.

Darüber hinaus möchte ich auch meinen ehemaligen Kollegen am Institut danken, mit denen ich stets eine angenehme Zeit verbringen durfte. Besonders hervorheben möchte ich die letzten anderthalb Jahre mit Patrick Diekhake, in denen wir uns bei unserem gemeinsamen Ziel, dem Abschluss unserer Dissertationen, unterstützt haben. Auch die Studierenden, deren Arbeiten ich betreuen durfte, haben mit den während der Betreuung geführten Gesprächen zum Erfolg dieser Arbeit beigetragen. Besonders erwähnen möchte ich dabei Jon-Conrad Linzmeier, der mir unermüdlich mit einer faszinierten Schnelligkeit und Genauigkeit zum Korrektur lesen zur Verfügung stand. Des Weiteren bedanke ich mich bei den Mitarbeiterinnen des Geschäftszimmers, die mir mit Rat und Tat zur Seite gestanden haben.

Der Karl-Vossloh-Stiftung danke ich für das Stipendium, welche mir in meinen letzten zwei Jahren am Institut die fokussierte Fertigstellung ermöglicht hat.

Mein besonderer Dank gilt meinen Eltern, die es mir ermöglicht haben, mich frei zu entfalten und so die Grundlage für meine Persönlichkeit und diese Arbeit zu legen. Zudem wäre ohne ihre – auch finanzielle – Unterstützung mein Werdegang und schließlich diese Arbeit nicht möglich gewesen.

Der Dank an meine Frau Katja und unsere Kinder Flora und Henry kann nicht groß genug sein, da sie viele Tage und Abende auf mich verzichten mussten und mich dennoch ihre tiefe und innige Liebe spüren ließen und lassen. Ich weiß Eure Geduld mit mir – insbesondere während dem Abschluss von „Papas Buch“ sehr zu schätzen! Daher widme ich Euch diese Arbeit.

Kurzfassung

Mit dieser Arbeit wird ein Beitrag zur Steigerung der Attraktivität des Schienenverkehrs durch den Wechsel von traditioneller streckenseitiger auf satellitenbasierte fahrzeugseitige Ortung geleistet. Hierbei wird eine Grundlage für den Entwicklungsprozess für die Selbstortung des Schienenfahrzeugs ohne streckenseitige Einrichtungen oder Aktivitäten des Fahrers erstellt, um die Zertifizierung und Typzulassung einer bordautonomen, mit ETCS Level 3 konformen satellitenbasierten Ortungseinheit für den Schienenverkehr zu erreichen.

Anstelle der momentan im Schienenverkehr üblichen diskreten Zugortung können mit Einführung der satellitenbasierten kontinuierlichen Ortung eine Vielzahl an Vorteilen durch einen effizienteren Betrieb und den Verzicht auf streckenseitige Ortungskomponenten sowie Signalisierung ermöglicht und realisiert werden.

Die hier konzipierte Ortungseinheit muss für eine Zertifizierung entsprechend dem gültigen normativen Rahmen entwickelt werden. Dafür werden der normative Rahmen und dessen historische Entwicklung analysiert und die beteiligten Organisationen im Normerstellungsprozess sowie die Entwicklungsprozesse in Europa betrachtet. Um die Ergebnisse dieser Arbeit auch weltweit für Entwicklungsprozesse nutzen zu können, wird auch der internationale normative Rahmen fokussiert. Darauf aufbauend soll die Begutachtung und Zertifizierung der satellitenbasierten Ortungseinheit im Schienenverkehr durchgeführt und der Prozess nachvollzieh- und wiederholbar dargestellt werden. Die satellitenbasierte Zugortung soll in moderne Zugbeeinflussungssysteme eingebunden werden und ist somit nicht separat einsetzbar. Für die somit notwendige Integration wird hier die Grundlage gelegt, die Umsetzung erfolgt durch ein modulares Modellkonzept für die Schnittstellen.

Um eine klar strukturierte Darstellung zu ermöglichen, wird ein terminologisch konsistentes Vorgehen eingeführt und genutzt. Der Fokus liegt dabei auf für die Entwicklung und Zertifizierung relevanten Termini, was zum Verständnis und für eine konsistente Durchführung notwendig ist. Dies ist die Basis für die sichere Systementwicklung und die damit verknüpfte Zertifizierung für ein System mit eindeutigen Systemgrenzen. Diese werden hier eingeführt und sind notwendig, um festzulegen, für welche Teile die Sicherheitsanalyse zutreffend und anzuwenden ist. Dieses Vorgehen ermöglicht es, frühzeitig Probleme und Schwierigkeiten zu erkennen, adäquate Lösungen zu erarbeiten und diese in den Entwicklungsprozess einbinden zu können. Die dafür erforderlichen Prozesse werden zunächst allgemein dargestellt und darauf aufbauend auf die Zertifizierung angewandt, die der Nutzung der satellitenbasierten Ortung im Schienenverkehr zugrunde liegt.

Abstract

This thesis contributes to a more attractive railways by enhancing the change from traditional track side to satellite based vehicle self-localisation. The development process for the self-localisation of a rail vehicle without track side infrastructure and activities of the driver is created to reach the certification and type approval of a board autonomous localisation unit for railways compatible with ETCS level 3.

Instead of the currently used discrete localisation in railways the advantages of satellite based localisation can be used for a continuous localisation. This leads to various benefits by an efficient operation and the abandonment of track side localisation as well as signalling components.

The localisation unit designed in this thesis has to be developed for a certification according the normative background which is therefore analysed. Furthermore the historical background of the normative background is analysed and the participating organisations in the creation of a norm as well as the development process in Europe are focused. To use the results of this work for worldwide development processes, the international normative background is focused as well. On this basis, the certification and assessment of the satellite based localisation unit for railways is carried out with consistent and comprehensive process. The satellite based train localisation is integrated in modern train control system and can therefore not be used separately. For the necessary integration the fundamental work is done, the implementation is carried out by a modular model concept for the interfaces.

To enable a clear structured description, a terminologically consistent approach is introduced and used. The focus is on the terms relevant for development and certification to enhance the comprehensibility and for a consistent implementation. This work is the basis for a safe system development and the connected certification with a clearly structured system. These are introduced here and are necessary to know the relevant parts for the safety analysis. This approach enables to identify potential problems and difficulties early and to adopt adequate solutions to be included in the development process. The necessary processes are introduced in general and subsequently applied to the certification of the satellite based localisation in railways.

Inhaltsverzeichnis

Vorwort III
Kurzfassung V
Abstract VI
Inhaltsverzeichnis VII
Verzeichnis der Abkürzungen und Akronyme XIII
Glossar XVII
1 Einleitung 1
1.1 Herausforderungen im Schienenverkehr und mögliche Potenziale 1
1.1.1 Interoperabilität des Schienenverkehrs in Europa 1
1.1.2 Wirtschaftlicher Betrieb von Nebenstrecken 2
1.1.3 Verzicht auf streckenseitige Infrastruktur 2
1.1.4 Erhöhung der Streckenkapazität 3
1.1.5 ETCS als europäisches Zugbeeinflussungssystem 3
1.1.6 Ansatz, Problemstellung 4
1.2 Abgrenzung der Arbeit und Vorarbeiten 5
1.3 Ziele dieser Arbeit 6
1.3.1 Teilziel A: Konsistente Darstellung der Systemarchitektur 7
1.3.2 Teilziel B: Sicherheitsgerichteter Entwicklungsprozess 8
1.3.3 Teilziel C: Nachweis der sicheren Funktionalität 8
1.4 Struktur dieser Arbeit 9
2 Stand der Forschung und Technik in Zugbeeinflussung und Ortung 11
2.1 Leitsysteme zur Steuerung des Verkehrssystems Eisenbahn 11
2.1.1 Einführung Zugbeeinflussungssysteme 11
2.1.2 Gliederung der Zugbeeinflussungssysteme 12
2.1.3 Entwicklung und Anwendung der Zugbeeinflussung in Europa 12
2.1.4 Wandel zur europäischen Zugbeeinflussung 14
2.1.5 Technische Umsetzung von ETCS 14
2.1.6 Nutzung von ETCS in Europa 15
2.2 Migrationsprozesse im Schienenverkehr 16
2.2.1 Durchführung der Migration 16
2.2.2 Prozess der Migration 17
2.2.3 Besonderheiten der Migration von Zugbeeinflussungssystemen 18
2.2.4 Migration zwischen verschiedenen ETCS Leveln 19
2.3 Ortung im Schienenverkehr 20
2.3.1 Klassifikation von Ortungsmethoden 21
2.3.2 Fahrzeugseitige kontinuierliche Ortung 21
2.3.3 Strukturierung der zur Ortung verwendeten Sensoren 22
2.3.4 Fahrzeugseitige Sensoren und digitale Karte 23

2.3.5 Stand der Nutzung von GNSS im Schienenverkehr 24
2.3.6 In Betrieb befindliche satellitenbasierte Zugbeeinflussungssysteme....25
2.3.7 Konzepte satellitenbasierter Zugbeeinflussungssysteme 26
2.4 Satellitenbasierte Sensorik 27
2.4.1 Satellitenbasierte Ortung....28
2.4.2 Funktionsweise und technische Aspekte der GNSS 29
2.4.3 Weltweite GNSS 30
2.4.4 Galileo....31
2.4.5 Erhöhung der Genauigkeit 32
2.4.6 Weltweite Ergänzungssysteme 33
2.4.7 Anwendungen der Luftfahrt....33
2.5 Integration und Zertifizierung der satellitenbasierten Ortung....35
2.5.1 Generische Zertifizierung satellitenbasierter Ortungssysteme 35
2.5.2 Domänenspezifische Zertifizierung satellitenbasierter Ortung....37
2.5.3 Zertifizierung industrieller Komponenten für den Schienenverkehr 37
3 Normativer Rahmen....39
3.1 Entwicklung normativer Dokumente 39
3.1.1 Beteiligte Organisationen am Normerstellungsprozess 40
3.1.2 Beteiligte Organisationen im Gesetzgebungsprozess 40
3.1.3 Beteiligte Interessenverbände 41
3.1.4 Wandel der europäischen Legislative 41
3.1.5 Wandel des sicherheitsgerichteten Entwicklungsprozesses....44
3.1.6 Einfluss des rechtlichen Wandels auf die Entwicklung und Zertifizierung 44
3.2 Zugrunde liegende Dokumente des normativen Rahmens....45
3.2.1 Allgemeine Industrienormen....46
3.2.2 Normen der Systemklassifikation 47
3.2.3 Grundlegende Normen des Schienenverkehrs 47
3.2.4 Grundlegende Spezifikationen des Schienenverkehrs 49
3.2.5 Dokumente des Herstellers und Betreibers....50
3.2.6 Internationale Dokumente der Entwicklung im Schienenverkehr 51
3.3 Sicherheitsnachweisführung....51
3.3.1 Begriffsdefinitionen 52
3.3.2 Sicherheitsnachweis in der Luftfahrt 54
3.3.3 Sicherheitsnachweis im Schienenverkehr in Europa 54
3.3.4 Einfluss der TSI auf Entwicklung und Zertifizierung....58
3.3.5 Sicherheitsnachweis im Schienenverkehr weltweit 58
3.3.6 Domänenübergreifender Ansatz 59
3.3.7 Strukturierung der Sicherheitsnachweisführung....60
3.3.8 Zusammenfassung der Ansätze....60
3.4 Normative Anforderungen im Schienenverkehr 61

3.4.1 Risikoakzeptanzkriterien im Schienenverkehr 62
3.4.2 Normative Anforderungen an Komponenten im Schienenverkehr 63
3.4.3 Normative Anforderungen an den Entwicklungsprozess 64
3.4.4 Normative Anforderungen an den Entwicklungsprozess (international) 65
3.4.5 Durchführung der sicheren Systementwicklung 67
3.4.6 Nachweiskonzeption 68
3.4.7 Normkonforme entwicklungsbegleitende Dokumentation 71
3.4.8 Inbetriebnahmegenehmigung 72
4 Entwicklung sicherer Systeme und Systemstrukturierung 73
4.1 Entwicklung technischer Systeme im Schienenverkehr 73
4.1.1 Generischer sicherheitsgerichteter Entwicklungsprozess 74
4.1.2 Domänenunabhängige Verantwortlichkeiten 75
4.1.3 Personelle und institutionelle Unabhängigkeiten nach Sicherheitsstufe 76
4.1.4 Verantwortlichkeiten im Entwicklungsprozess 77
4.1.5 Verantwortlichkeiten während der Zertifizierung 79
4.2 Grundlagen der Strukturierung eines technischen Systems 81
4.2.1 Herausforderungen der Systemstrukturierung 82
4.2.2 Grundlegende Definitionen 82
4.2.3 Eigenschaften des Systembegriffs 83
4.2.4 Bedeutende Aspekte der Erstellung der Systemarchitektur 84
4.3 Ansätze zur Durchführung der Systemstrukturierung 84
4.3.1 Funktionsbezogene Struktur 85
4.3.2 Produktbezogene Struktur 87
4.3.3 Ortsbezogene Struktur 88
4.3.4 Integrierte Struktur 90
5 Strukturierung der Anforderungsspezifikationen 91
5.1 Anforderungen an Betrieb und Instandhaltung 91
5.1.1 Generische Darstellung der Anforderungen an Anwendungen 91
5.1.2 Strukturierung der Funktionen im Schienenverkehr 92
5.1.3 Zusammenfassung 95
5.2 Anforderungen an Stilllegung und Entsorgung 96
5.3 Anforderungen an Betrieb mit externen Einflüssen 96
6 Strukturierung der Sicherheitsanforderungsspezifikationen 97
6.1 Aufstellen der Sicherheitsanforderungen 98
6.1.1 Anforderungen an Systemkomponenten 99
6.1.2 Anforderungen entsprechend des Funktionsaspekts 100
6.1.3 Resultierende Anforderungen an die Ortungseinheit 102
6.1.4 Anforderungen an den Entwicklungsprozess 105
6.1.5 Anforderungen an durch Sensoren gelieferte Informationen 105

6.1.6 Technische Sicherheitsanforderungen 105
6.2 Anforderungen an Sicherheitsüberwachung im Betrieb 106
6.3 Anforderungen an Stilllegung und Entsorgung 106
6.4 Anforderungen an Sicherheitserprobung 106
7 Erstellung des Sicherheitsnachweises 109
7.1 Definition des Systems 110
7.1.1 Einleitung 111
7.1.2 Systemarchitektur 112
7.1.2.1 Beschreibung der Systemarchitektur 113
7.1.2.2 Definition der Schnittstellen 116
7.1.3 Sichere Systementwicklung 119
7.1.3.1 Zusammenfassung der technischen Sicherheitsprinzipien 119
7.1.3.2 Projektierung von Teilsystemen und Systemaufbau 123
7.2 Allgemeine Informationen 124
7.2.1 Qualitätsmanagementbericht 124
7.2.2 Sicherheitsmanagementbericht 124
7.3 Technische Sicherheitsanalyse und Umsetzung 124
7.3.1 Einleitung 125
7.3.2 Betrieb mit externen Einflüssen 126
7.3.2.1 Klimatische Bedingungen 126
7.3.2.2 Mechanische Bedingungen 126
7.3.2.3 Höhe über Meeresspiegel 126
7.3.2.4 Elektrische Bedingungen (nicht auf Fahrzeugen) 127
7.3.2.5 Elektrische Bedingungen (auf Fahrzeugen) 127
7.3.2.6 Schutz vor unberechtigtem Zutritt 127
7.3.2.7 Erschwerte Bedingungen 127
7.3.3 Ausfallauswirkungen 127
7.3.3.1 Angabe der Fail-Safe-Prinzipien 128
7.3.3.2 Unabhängigkeit von Betrachtungseinheiten 129
7.3.3.3 Schutz gegen systematische Fehler 130
7.3.3.4 Auswirkung von Einzelausfällen 130
7.3.3.5 Auswirkung von Mehrfachausfällen 131
7.3.3.6 Offenbarung von (Einzel-)Ausfällen 132
7.3.3.7 Aktion nach Ausfalloffenbarung 132
7.3.4 Nachweis des korrekten funktionalen Verhaltens 132
7.3.4.1 Erfüllung der Sicherheitsanforderungen 133
7.3.4.2 Nachweis der korrekten Hardwarefunktionalität 135
7.3.4.3 Nachweis der korrekten Softwarefunktionalität 136
7.3.5 Sicherheitsbezogene Anwendungsbedingungen 137
7.3.5.1 Betrieb und Instandhaltung 138
7.3.5.2 Sicherheitsüberwachung im Betrieb 138

7.3.5.3 Stilllegung und Entsorgung....139
7.3.6 Sicherheitserprobung....139
7.3.6.1 Erfüllung der Systemanforderungen....139
7.3.6.2 Ergebnisse....140
7.4 Zusammenfassung und Schlussfolgerung....140
7.4.1 Beziehungen zu anderen Sicherheitsnachweisen....140
7.4.2 Zusammenfassung....141
8 Sicherheitsgutachten....143
8.1 Begutachtungsgegenstand....143
8.2 Unabhängigkeit des Gutachters....143
8.3 Durchführung der Begutachtung....144
8.4 Dokumentation der Begutachtung....145
8.5 Abweichungen gegenüber Sicherheitsanforderungen....147
8.6 Zulassung des betrachteten Systems....148
9 Zusammenfassung und Ausblick....149
9.1 Zusammenfassung und kritische Diskussion der Ergebnisse....149
9.2 Ausblick....150
Anhang 1: Projekte zur satellitenbasierten Ortung im Schienenverkehr....151
Anhang 2: Bekannte ETCS Ausrüstung in Europa....152
Anhang 3: Normativer Rahmen der satellitenbasierten Ortung....153
Anhang 4: Strukturierung der Funktionen in anderen Verkehrsdomänen....154
Anhang 5: Anforderungen an Komponenten in Schienenfahrzeugen....155
Literaturverzeichnis....156
Abbildungsverzeichnis....169
Tabellenverzeichnis....172

Verzeichnis der Abkürzungen und Akronyme

ACM	Axel Counter Module
AEG	Allgemeines Eisenbahngesetz
ALARP	as low as reasonably practicable (so niedrig, wie vernünftigerweise praktikabel)
ANCS	Advanced Network Control System
APV	Approach procedures with Vertical Guidance (Anflugverfahren mit vertikaler Führung)
AssBo	Assessment bodies (unabhängige Bewertungsstelle – UBS)
ATMS	Advanced Train Management System
AWS	Automatic Warning System (britisches Zugbeeinflussungssystem)
BMVI	Bundesministerium für Verkehr und digitale Infrastruktur
CCS	Control command and signalling (Zugsteuerung, Zugsicherung und Signalgebung)
CEN	Comité Européen de Normalisation (Europäisches Komitee für Normung)
CENELEC	Comité Européen de Normalisation Électrotechnique (Europäisches Komitee für elektrotechnische Normung)
COTS	Components Off The Shelf (industrielle Komponenten)
CPU	Central Processing Unit (Prozessor)
CSM	Common Safety Methods (gemeinsame Sicherheitsmethoden)
CST	Gemeinsame Sicherheitsziele (Common Safety Targets)
CWAS	Canada Wide Area Augmentation System
DAkkS	Deutsche Akkreditierungsstelle
DB	Deutsche Bahn
DeBo	Designated Body (benannte beauftragte Stelle – BSS)
DIN	Deutsches Institut für Normung
DKE	Deutsche Kommission Elektrotechnik Elektronik Informationstechnik
DOT	Department of Transportation
EBA	Eisenbahn-Bundesamt
EBO	Eisenbahn-Bau- und Betriebsordnung
EBuLa	Elektronischer Buchfahrplan und Langsamfahrstellen
EC	European Commission (Europäische Kommission)
EGNOS	European Geostationary Navigation Overlay Service (europäisches Erweiterungssystem zur satellitenbasierten Ortung)
EIU	Eisenbahninfrastrukturunternehmen
ELSS	Eisenbahnleit- und Sicherungstechnik

EMV	Elektromagnetische Verträglichkeit
EN	Europäische Normen
ERA	European Railway Agency (Europäische Eisenbahnagentur)
ERTMS	European Rail Traffic Management System (System für Management und Steuerung des Eisenbahnverkehrs auf den Strecken der TEN)
ETCS	European Train Control System (Europäisches Zugbeeinflussungssystem)
ETML	European Train Management Layer (Europäisches Zugmanagementsystem)
ETSI	European Telecommunications Standards Institute (Europäisches Institut für Telekommunikationsnormen)
EU	Europäische Union
EUROCONTROL	European Organisation for the Safety of Air Navigation (Europäische Organisation zur Sicherung der Luftfahrt)
EVC	European Vital Computer (Steuerungsgerät für den Schienenverkehr)
EVU	Eisenbahnverkehrsunternehmen
FMEA	Failure Mode and Effects Analysis (Fehlermöglichkeits- und -einflussanalyse)
FMECA	Failure Mode, Effects, and Criticality Analysis (Fehlermöglichkeits-, Kritizitäts- und -einflussanalyse)
FRA	Federal Railroad Administration
GAGAN	GPS Aided Geo Augmented Navigation
GaLoROI	Galileo Localisation for Railway Operation Innovation
GAMAB	Globalement au moins aussi bon (Mindestens genauso gut)
GBAS	Ground Based Augmentation System (bodengestütztes Ergänzungssystem)
GLONASS	ГЛОбальная Навигационная Спутниковая Система (Globales satellitenbasiertes Ortungssystem)
GNSS	Global Navigation Satellite System (globales satellitenbasiertes Ortungssystem)
GPS	Global Positioning System (globales Positionierungssystem)
GSM-R	Global System for Mobile Communications – Rail(way) (Mobilfunksystem für den Einsatz im Schienenverkehr)
GSN	Goal Structuring Notation (zielstrukturierende Beschreibung)
ICAO	International Civil Aviation Organisation (Internationale Zivilluftfahrtorganisation)
IEC	Internationale Elektrotechnische Kommission
IEEE	Institute of Electrical and Electronics Engineers (weltweiter Berufsverband von Ingenieuren)
IGS	ziviler Internationaler GNSS Service
IRIS	International Railway Industry Standard

ISO	International Organisation for Standardisation (Internationale Organisation für Normung)
ITCS	Incremental Train Control System (inkrementelles Zugbeeinflussungssystem)
ITU	International Telecommunication Union (internationale Fernmeldeunion)
iVA	Institut für Verkehrssicherheit und Automatisierungstechnik der TU Braunschweig
JRU	Juridical Recording Unit
KML	Keyhole Markup Language (XML-basierte Sprache zur Programmierung)
LZB	Linienförmige Zugbeeinflussung
MEM	Minimum Endogenous Mortality (Minimale Endogene Mortalität)
MOTS	Modifiable off-the-shelf (modifizierte Industriekomponenten)
MSAS	Multi-Functional Satellite Augmentation System
MTBF	Mean Time Between Failures (mittlere Lebenszeit)
NNTR	Notified National Technical Rules (notifizierte nationale technische Regeln)
NoBo	Notified Body (benannte Stelle – BS)
NPA	Non-precision Approach (Unpräziser Anflug)
NSA	National Safety Authority (nationale Sicherheitsbehörde – NSB)
ÖBB	Österreichische Bundesbahnen
OEM	Original Equipment Manufacturer (Erstausrüster)
PTC	Positive Train Control
PZB	Punktförmige Zugbeeinflussung
QMS	Qualitätsmanagementsystem
QZSS	Quasi Zenith Satelliten System
railML	Datenaustauschformat im Schienenverkehrssektor
RAMS	Reliability, Availability, Maintainability, Safety (technische Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit, Sicherheit)
RFID	Radio-Frequency Identification (Identifizierung mit Hilfe elektromagnetischer Wellen)
RPZ	Risikoprioritätszahl
SATLOC	Satellite based operation and management of local low traffic lines
SATNAB	Satellitennavigationsgestütztes Navigations-Bodenexperiment
SatZB	Satellitenbasierte Zugbeeinflussung
SBAS	Satellite Based Augmentation System (satellitenbasiertes Ergänzungssystem)
SDKM	система дифференциальной коррекции и мониторинга (System zur differentiellen Korrektur und Überwachung)

SIRF	Sicherheitsrichtlinie Fahrzeug
SMS	Sicherheitsmanagementsystem
SNAS	Satellite Navigation Augmentation System
SPS	Speicherprogrammierbare Steuerung
SRS	System Requirement Specification
SIL	Safety Integrity Level (Sicherheitsintegritätslevel)
STAMP	Systems-Theoretic Accident Model and Processes
STM	Specific Transmission Module (spezifisches Übertragungsmodul)
TCM	Track Circuit Modul
TEIV	Transeuropäische Eisenbahn Interoperabilitätsverordnung
TEN	Transeuropäische Netze
TeSip	Technischen Sicherheitsplans Fahrzeug
THR	Tolerable Hazard Rate (tolerierbare Gefährdungsrate)
TSI	Technical Specifications for Interoperability (Technischen Spezifikationen für Interoperabilität)
TTFF	Time to first fix (Zeit bis zur ersten Positionsbestimmung)
UIC	Union internationale des chemins de fer (Internationaler Eisenbahnverband)
UML	Unified Modeling Language (vereinheitlichte Modellierungssprache)
UNIFE	Union des Industries Ferroviaires Européennes (Verband der europäischen Eisenbahnindustrie)
UNISIG	Union Industry of Signalling (Arbeitsgruppe der UNIFE)
USA	United States of America Vereinigte Staaten von Amerika
VDV	Verband Deutscher Verkehrsunternehmen
WAAS	Wide Area Augmentation System
WGS	World Geodetic System
XML	Extensible Markup Language (erweiterbare Auszeichnungssprache)
ZLB STH	Zugleitbetrieb Stern & Hafferl

Glossar

„ORTUNG ist die Bestimmung des Bewegungszustands eines bestimmten Verkehrsmittels (d. h. Position, Geschwindigkeit nach Betrag und Richtung bezogen auf einen Bezugspunkt des Verkehrsmittels) in einem Bezugssystem.“ [Schnieder 2012]

„Der SICHERHEITSNACHWEIS ist ein dokumentierter Nachweis darüber, dass ein Produkt die gesetzlichen und spezifizierten Sicherheitsanforderungen erfüllt.“ [Schnieder/Schnieder 2013]

Ein SCHIENENFAHRZEUG ist ein „spurgebundenes Fahrzeug, das auf Gleisen geführt und getragen wird.“ [DIN EN 15380-1]

ANFORDERUNGEN sind „notwendige Bedingung oder Vermögen, um die Lösung einer Aufgabe oder eines Zieles einzuschränken.“ [DIN EN 15380-5; DIN EN 15380-4]

INFRASTRUKTUR ist ein „System von Einrichtungen, Ausrüstungen und Dienstleistungen, das für den Betrieb einer Organisation erforderlich ist.“ [DIN EN ISO 9000]

Ein PROZESS ist die „Gesamtheit von aufeinander einwirkenden Vorgängen in einem System, durch die Material, Energie oder Information umgeformt, transportiert oder gespeichert wird.“ [DIN EN 81346-1]

Ein SYSTEM ist eine Einheit, die „als solches erkennbar ist und in der Lage ist, sich gegen äußere Einflüsse dauerhaft zu erhalten und aus sich heraus bestimmte Zwecke zu erfüllen.“ [Schnieder/Schnieder 2010]

Ein OBJEKT ist eine „Betrachtungseinheit, die in einem Prozess der Entwicklung, Realisierung, Betriebs-, und Entsorgung behandelt wird.“ [DIN EN 81346-1]

„Eine FUNKTIONSBEZOGENE STRUKTUR basiert auf dem Zweck eines Systems. Sie zeigt die Untergliederung eines Systems in Bestandteilobjekte im [sic] Bezug auf den Funktionsaspekt, ohne dabei mögliche Orts- und/oder Produktaspekte dieser Objekte zu berücksichtigen.“ [DIN EN 81346-1]

„Eine PRODUKTBEZOGENE STRUKTUR basiert auf der Art und Weise, wie ein System realisiert, aufgebaut oder geliefert wird, wobei Zwischenkomponenten oder endgültige Komponenten verwendet werden. Eine produktbezogene Struktur zeigt die Untergliederung eines Systems in Bestandteilobjekte im Hinblick auf den Produktaspekt, ohne mögliche Funktions- und/oder Ortsaspekte dieser Objekte zu berücksichtigen.“ [DIN EN 81346-1]

„RISIKO ist die Wahrscheinlichkeit des Auftretens einer Gefahr, die einen Schaden verursacht und der Schweregrad des Schadens.“ [DIN EN 50126]

„Die Hauptaufgabe eines EISENBAHNLEIT- UND SICHERUNGSSYSTEMS (ELSS) ist die Vermeidung von Unfällen und gefährlichen Situationen. Daraus resultiert fast zwangsläufig, dass alle ELSS eine mehr oder weniger ähnliche Funktionalität haben, so z. B. die Sicherung der Fahrstraße oder die Überwachung der Fahrgeschwindigkeit. Auf der Basis der Klassifikationen möglicher Gefährdungen und Funktionen zu ihrer Vermeidung werden die generischen Funktionen von ELSS gesammelt.“ [Meyer zu Hörste 2004]

„ZUGBEEINFLUSSUNGSSYSTEME sind Anlagen, die Informationen über die zulässige Fahrweise vom Fahrweg zum Fahrzeug übertragen und bei Abweichungen von der zulässigen Fahrweise auf dem Fahrzeug entsprechende Schutzreaktionen (in der Regel Zwangsbremsungen) auslösen. Je nach technischer Ausstattung wirken Zugbeeinflussungssysteme entweder nur als Ergänzung des ortsfesten Signalsystems oder ermöglichen eine Führung des Zuges nach Führerraumanzeigen unter Verzicht auf ortsfeste Signale.“ [Pachl 2013]

1 Einleitung

In dieser Arbeit wird die Grundlage für die Zertifizierung und Nachweisführung zur Typzulassung einer bordautonomen, mit dem europäischen Zugbeeinflussungssystem (European Train Control System – ETCS) konformen satellitenbasierten Ortungseinheit für den Schienenverkehr gelegt. Einleitend werden dafür als Motivation in Abschnitt 1.1 Herausforderungen im Schienenverkehr und Potenziale bei der Nutzung der satellitenbasierten Ortung sowie erste Lösungsansätze dargestellt. In Abschnitt 1.2 findet die Abgrenzung dieser Arbeit zu den Vorarbeiten statt, darauf aufbauend werden in Abschnitt 1.3 die Ziele und in Abschnitt 1.4 die Struktur dieser Arbeit dargestellt.

1.1 Herausforderungen im Schienenverkehr und mögliche Potenziale

Zugbeeinflussungssysteme in Europa befinden sich in einem Prozess des Wandels mit dem Ziel europäischer Harmonisierung. Dieser Wandel ist aufgrund der gewünschten Interoperabilität zwischen den Nationalstaaten, der Erschließung vieler ländlicher Regionen durch den Schienenverkehr und des hohen Kapazitätsbedarfs auf Strecken des Transeuropäischen Netzes (TEN) notwendig. Diese Aspekte sind zusammen mit der Entwicklung von ETCS motivierende Grundlage dieser Arbeit.

Einleitend wird in Abschnitt 1.1.1 die Interoperabilität des Schienenverkehrs in Europa betrachtet, in Abschnitt 1.1.2 wird der wirtschaftliche Betrieb von Nebenstrecken fokussiert. Die Darstellung, weshalb fahrzeugseitige anstatt streckenseitiger Ortung genutzt werden sollte, erfolgt in Abschnitt 1.1.3. In Abschnitt 1.1.4 wird zunächst die Erhöhung der Streckenkapazität thematisiert und im darauf folgenden Abschnitt 1.1.5 die mögliche Nutzung der satellitenbasierten Ortung für ETCS. Schließlich werden in Abschnitt 1.1.6 der Ansatz bzw. die Problemstellung dieser Arbeit erläutert.

1.1.1 Interoperabilität des Schienenverkehrs in Europa

Seitens der Europäischen Union (EU) wurden und werden viele Maßnahmen getroffen, um den grenzüberschreitenden Schienenverkehr zu harmonisieren. So wurden die permanent aktualisierten Technischen Spezifikationen für Interoperabilität (TSI) [EU/2008/57] erlassen, die zunächst den grenzüberschreitenden Verkehr auf den TEN erleichtern sollen. Um dieses Ziel nach aktuellem Stand der Technik zu erreichen, ist eine Harmonisierung von streckenseitiger und fahrzeugseitiger Technik notwendig. Bei Einsatz der satellitenbasierten Ortung wäre aufgrund des Verzichts auf streckenseitige Ausrüstungskomponenten abgesehen von verschiedenen Spurweiten lediglich die Harmonisierung der fahrzeugseitigen Technik erforderlich.

1.1.2 Wirtschaftlicher Betrieb von Nebenstrecken

Die Mitgliedsstaaten der EU zuzüglich Schweiz und Norwegen verfügen derzeit über ein Schienennetz von 223.000 km [UIC 2013] von denen etwa 118.000 km [EC 2013a] Nebenstrecken sind. Diese sind teilweise nicht wirtschaftlich zu betreiben und daher von einer Stilllegung bedroht – in Deutschland wurden bspw. 5.134 km des Streckennetzes seit 1994 stillgelegt, 93 % davon bis 2004 [EBA 2013]. Somit besteht besonders auf Nebenstrecken ein hoher Bedarf an kosteneffizientem und für den Fahrgast attraktivem Betrieb, um sie durch Eisenbahnverkehrsunternehmen (EVU) und Eisenbahninfrastrukturunternehmen (EIU) wirtschaftlich betreiben zu können. Fahrzeugseitig wurden durch den Einsatz von Leichttriebwagen anstelle von lokbespannten Zügen bereits Kosteneinsparungen erzielt [Reinhardt 2011].

Mit einer Modernisierung könnten Nachteile bestehender Zugbeeinflussungssysteme, die möglicherweise als Hemmnis für Innovationen wirken, beseitigt werden. Bezogen auf den Fahrzeugpark in der EU, Norwegen und der Schweiz von 63.500 Lokomotiven und Triebwagen, 107.000 Personenwagen und 732.000 Güterwagen [EC 2012] ergibt sich eine breite Anwendungsmöglichkeit der Ortungseinheit.

1.1.3 Verzicht auf streckenseitige Infrastruktur

Neben den beschriebenen fahrzeugseitigen Maßnahmen wird die Wirtschaftlichkeit im Schienenverkehr, insbesondere auf Nebenstrecken, von Kosten der streckenseitigen Signalisierung und Ortungskomponenten wie Achszählern negativ beeinflusst. Diese Einrichtungen müssen intensiv gewartet sowie instandgehalten werden und sind Witterung und Vandalismus ausgesetzt. Bei vergleichsweise wartungsarmen Sensoren wie RFID (Radio-Frequency Identification) oder Balisen ist zu beachten, dass diese zwar geringere Herstellungskosten als bspw. die Systeme Punktförmige Zugbeeinflussung (PZB) oder Linienförmige Zugbeeinflussung (LZB) haben, jedoch nur eingesetzt werden können, wenn sie an einer kartografisch bestimmten Stelle im Gleis verlegt sind und über die gesamte Lebenszeit dort verbleiben. Bei der Installation und bei Gleisarbeiten ist somit ein zeit- und kostenintensives Einmessen notwendig. Bei Gleis- und Schotterarbeiten besteht die Gefahr, dass die streckenseitigen Einrichtungen an eine andere Stelle versetzt werden und somit nicht mehr der vorher eingemessenen Position entsprechen. Zudem haben die bestehenden Zugbeeinflussungssysteme den Nachteil, dass zwar streckenseitige Einrichtungen ein Schienenfahrzeug lokalisieren, jedoch zunächst nicht bekannt ist, um welches Schienenfahrzeug es sich handelt. Erst durch Verknüpfung mit den Dispositionsdaten findet eine Ortung des Zuges statt, weswegen diese nur bedingt zur Ortung eines Zuges geeignet sind.

Mit dem Verzicht auf streckenseitige Infrastruktur wird die Sicherungsintelligenz auf das Fahrzeug verlagert, womit verschiedene Rationalisierungen erreicht werden können. Die Kosten des EVU steigen damit geringfügig, die des EIU sinken wesentlich [Thiele 2008; May 2010]. Bei Erneuerung der strecken- und fahrzeugseitigen Technik ist davon auszugehen, dass die Beteiligten erst langfristig von einer Migration zu einem neuen Zugbeeinflussungssystem profitieren [Bikker/Schroeder 2002]. Für die erfolgreiche Abwicklung des gesamten Prozesses ist eine intensive Abstimmung zwischen den beteiligten Institutionen, in diesem Fall zwischen Hersteller der Leit- und Sicherungstechnik, Betreiber (EVU, EIU), dem Gutachter, der Sicherheitsbehörde sowie der Öffentlichkeit notwendig.

1.1.4 Erhöhung der Streckenkapazität

Eine Vielzahl der weltweiten Strecken wird mit blockbasierten Zugbeeinflussungssystemen betrieben, wobei die Blöcke bis zu 20 km lang sein können [ARA 2009], was deren Kapazität stark einschränkt. In Deutschland sind die Blockabstände meist wesentlich kürzer, dennoch kann die Kapazität des deutschen Schienennetzes durch eine Optimierung der Leit- und Sicherungstechnik um 20 Mrd. tkm erhöht werden [Holzhey 2010], was ca. 20 % der Transportleistung des deutschen Schienennetzes entspricht [DIW 2014]. Die Steigerung der Kapazität würde eine höhere Wettbewerbsfähigkeit und somit einen höheren Marktanteil ermöglichen. Um die dafür notwendigen Optimierungen durchführen zu können, ist eine derzeit nicht gegebene Innovationskraft im Schienenverkehr notwendig [Klinge 1998].

Eine mögliche Innovation zur Erhöhung der Kapazität im Schienenverkehr ist ein verändertes Abstandshalteverfahren [Schnieder 2007]. So ermöglicht das Abstandshalteverfahren des Fahrens im beweglichen Raumabstand (Moving Block) eine etwa doppelt so hohe Kapazität im Vergleich zur Abstandshaltung in Blockabschnitten, die jeweils aus ein Kilometer langen Blöcken bestehen [Slovak 2006]. Dazu ist eine kontinuierliche anstatt einer diskreten Ortung notwendig, um den Zeitraum, in dem ein Fahrwegabschnitt besetzt ist, zu reduzieren, was durch satellitenbasierte Ortung unterstützt und realisiert werden kann.

1.1.5 ETCS als europäisches Zugbeeinflussungssystem

In einigen europäischen Ländern, bspw. im Vereinigten Königreich, sind bereits Verbesserungen der Leit- und Sicherungstechnik geplant [Thomas et al. 2008]. Dies kann durch ETCS gewährleistet werden. Für die Nutzung von ETCS sind fahrzeug- und streckenseitige Komponenten notwendig, es sind bspw. drei bis zwölf Balisen pro

Kilometer Gleis zu installieren [Pisek 2014; Beyer/Fußy 2014]. Auf Hochgeschwindigkeitsstrecken betragen die Gesamtkosten für Signaltechnik bei ETCS Level 2 ca. 300.000 Euro pro Kilometer [Yarman 2015]. Diese Kosten können sich während Erprobung und Betrieb erhöhen. Weitere Kosten entstehen bspw. durch die Nachrüstung von Balisengruppen vor Blocksignalen, was in Österreich aufgrund winterlichen Problemen mit der Hodometrie[1] notwendig war [Pisek 2014]. Weiterhin wirken sich die Vorteile von ETCS erst im fortgeschrittenen Verlauf des Lebenszyklus aus, da der Implementierungsaufwand sehr hoch ist. Die daraus resultierende verhaltene Akzeptanz ist ein Hemmnis für die Einführung von ETCS und führt dazu, dass die technische und betriebliche Interoperabilität bei ETCS nur iterativ erreicht werden kann [Leining 2014]. An dieser Stelle bietet eine satellitenbasierte Ortungseinheit wesentliche Vorteile, da lediglich eine fahrzeugseitige Einrichtung notwendig ist und somit keine Interaktionen mit der Strecke betrachtet werden müssen. Nach Abschluss der Entwicklung der Ortungseinheit kann diese unabhängig von der Leit- und Sicherungstechnik direkt auf dem Fahrzeug installiert und eingesetzt werden.

1.1.6 Ansatz, Problemstellung

Die Erhöhung der Kapazität von Strecken kann unter anderem durch ein traditionelles Zugbeeinflussungssystem mit hohem Automatisierungsgrad oder durch eine kontinuierliche Ortung erfolgen. Ein automatisierter Betriebsablauf führt zu Kosteneinsparungen, jedoch sind die notwendigen Investitionen erst bei einer hohen Auslastung wirtschaftlich vertretbar [May 2010]. Somit kann mit diesem Ansatz lediglich die Kapazität auf Hauptstrecken erhöht werden. Jedoch bietet er keine Lösung für Nebenstrecken aufgrund der dortigen vergleichsweise geringen Zugdichte und aufgrund des hohen technischen Harmonisierungsaufwands nur bedingt eine Lösung für die Interoperabilität zwischen den Nationalstaaten Europas. Die satellitenbasierte Ortung der Züge bietet sich hingegen als Lösung an, da sie eine kontinuierliche fahrzeugseitige Ortung der Züge ermöglicht und deutlich geringere Investitionen verlangt. Bereits 2006 wird daher in einem Positionspapier der EU ausgeführt, dass „die Satellitennavigation (…) dazu bestimmt (ist), den Eisenbahnsektor zu revolutionieren“ [EC 2006]. Dabei kann die satellitenbasierte Ortung neben einer kostengünstigeren Ortung und damit Zugbeeinflussung auf Nebenstrecken auch durch die Implementierung in ETCS die Interoperabilität des Schienenverkehrs unterstützen und die Kapazität auf bestehenden Strecken erhöhen.

[1] Entgegen der üblicheren Schreibweise „Odometer“ bzw. Odometrie wird in dieser Arbeit die entsprechend dem deutschen Duden korrekte Schreibweise „Hodometer“ bzw. „Hodometrie“ verwendet.

Die Anwendung der satellitenbasierten Ortung kann mit ETCS kombiniert werden, was sich speziell in Level 3 anbietet, da dort auf streckenseitige Infrastruktur verzichtet werden soll und die Position und Vollständigkeit des Zuges trotzdem möglichst genau bekannt sein muss.

1.2 Abgrenzung der Arbeit und Vorarbeiten

Erste Ansätze zur sicherheitsrelevanten Nutzung satellitenbasierter Ortungssysteme (Global Navigation Satellite System – GNSS) im Schienenverkehr wurden in nationalen und internationalen Forschungsprojekten mit dem Ziel der Anwendung auf Nebenstrecken untersucht [Bikker/Schroeder 2002; Marais 2002; Schnieder/Barbu 2009; Poliak 2009; May 2010; Stadlmann et al. 2012] und die Genauigkeit sowie Verfügbarkeit nachgewiesen [DemoOrt 2009; Alcouffe/Barbu 2001]. Eine Übersicht der abgeschlossenen und zum Teil laufenden Projekte ist in Anhang 1 dargestellt, die genutzten Arbeiten und die entsprechende Abgrenzung ist in Abbildung 1-1 abgebildet.

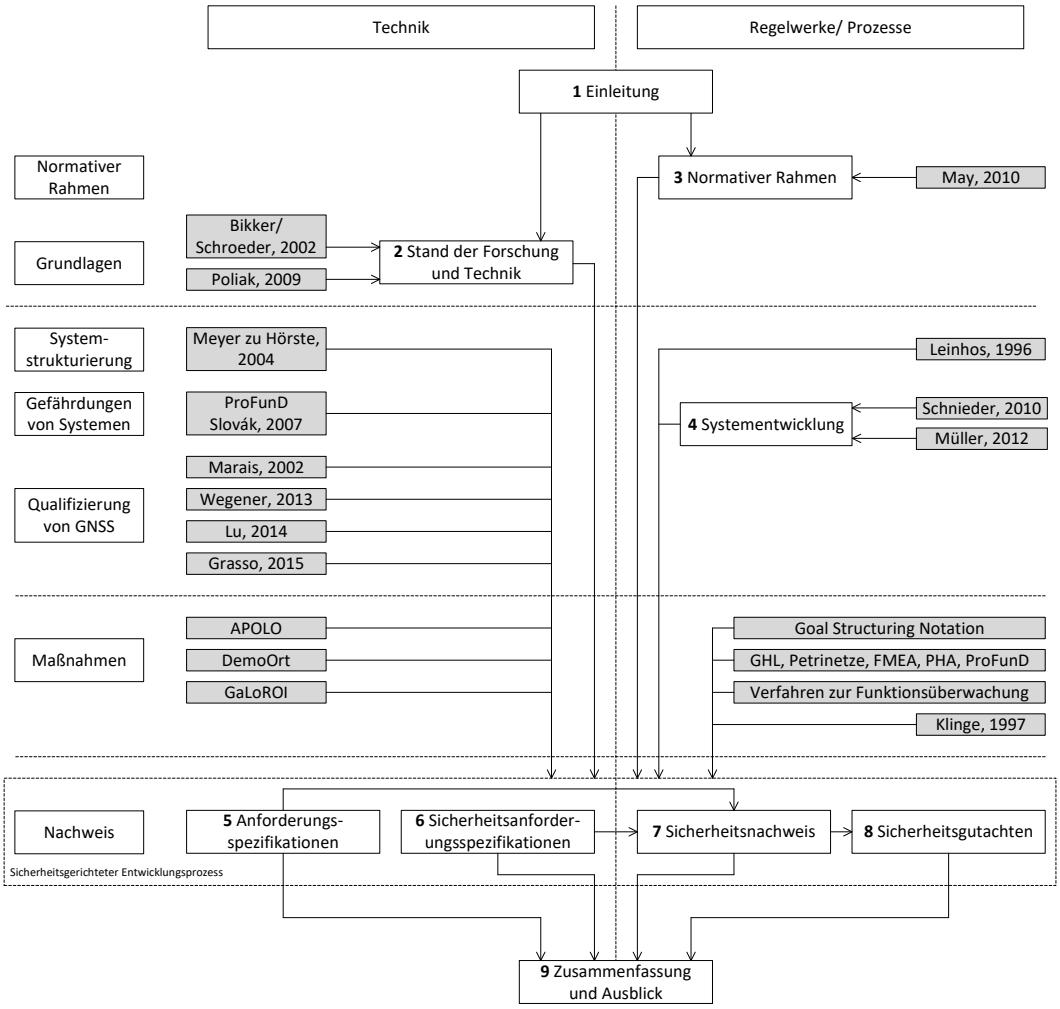


Abbildung 1-1: Abgrenzung zu anderen Arbeiten und genutzte Vorarbeiten

In den dargestellten Projekten und Arbeiten wurde das Potenzial der satellitenbasierten Ortung für sicherheitsrelevante Anwendungen beschrieben [Thomas et al. 2008]. In den vorangegangenen Projekten ist die entsprechende Entwicklung jedoch nicht über den Prototypenstatus hinausgegangen. Eine Auswahl der genutzten Arbeiten und die entsprechende Abgrenzung ist in Abbildung 1-1 dargestellt. Genutzte Vorarbeiten sind dabei grau hinterlegt, die Umsetzung wird in der Struktur der Arbeit in Abschnitt 1.4 dargestellt. Die Vorarbeiten werden in dieser Arbeit insbesondere zur Erstellung des sicherheitsgerichteten Entwicklungsprozesses aufgegriffen, der in den Kapiteln 5, 6, 7 und 8 erstellt wird. Daraus ergeben sich die in dieser Arbeit zu betrachtenden Aspekte.

Die Nutzung von Ergebnissen vorheriger Arbeiten erfolgt mit sinnvollen Erweiterungen. So wird in [May 2010] der Fokus auf ursächlich im Schienenverkehr entstehende Gefährdungen, also auf den Unfalltyp Kollision, gelegt. Als Erweiterung zu [May 2010] wird in dieser Arbeit auch die Unfallart Entgleisung fokussiert. Zudem werden mögliche Unfälle durch Umwelteinflüsse, die nach [May 2010] nicht ursächlich durch das Ortungssystem hervorgerufen werden können, betrachtet, da hier davon ausgegangen wird, dass Umwelteinflüsse durchaus einen Einfluss auf die Ortung haben.

1.3 Ziele dieser Arbeit

In dieser Arbeit wird ein Beitrag zur Steigerung der Rolle des Schienenverkehrs als nachhaltiges Rückgrat der Verkehrsinfrastruktur geleistet. Bereits heute hat der Schienenverkehr eine wichtige Rolle durch seine Kernaufgabe, den pünktlichen und sicheren Transport von Personen und Gütern in großen Mengen mit einem hohen Niveau an Sicherheit und Transportgeschwindigkeit durchzuführen. Dazu sind effiziente Systeme zur Leitung und Sicherung einer Zugfahrt notwendig, die in dieser Arbeit mit dem Entwurf eines Entwicklungs- und Zertifizierungsprozesses für eine sichere und präzise kontinuierliche Ortung erstellt werden. Diese soll ausschließlich durch fahrzeugseitige Ortung realisiert werden, die auf Strecken genutzt werden kann, auf denen das bestehende Zugbeeinflussungssystem derzeit oder zukünftig nicht mehr den organisatorischen, betrieblichen, wirtschaftlichen oder sicherheitsrelevanten Anforderungen entspricht. Weiterhin ist auf dem TEN [EU/2008/57] und auf neu zugelassenen Schienenfahrzeugen [EU/2014/1302] die Einführung von ETCS durch die EU vorgeschrieben, was den Bedarf nach einer präzisen Ortung für eine effiziente Zugbeeinflussung verdeutlicht.

Um den Einsatz von GNSS im Schienenverkehr und somit den Verzicht auf streckenseitige Einrichtungen zu ermöglichen, ist die Zertifizierung der Sicherheit, Präzision, Richtigkeit und Zuverlässigkeit der berechneten Positionsinformation

notwendig. Im Straßen-, Luft- und Schiffsverkehr gibt es bereits erste Ansätze, die jedoch noch nicht zu einer weit verbreiteten Anwendung über die jeweilige Verkehrsdomäne hinaus geführt haben. Dem gegenüber stehen zertifizierte satellitenbasierte Anflugverfahren im Flugverkehr. Diese Arbeit soll unter Nutzung vorhandener Erkenntnisse vergleichbare Voraussetzungen für den Schienenverkehr schaffen.

Die Teilziele, welche für eine sichere Entwicklung und Zertifizierung der satellitenbasierten Ortungseinheit ohne streckenseitige Infrastruktur im Schienenverkehr notwendig sind, werden in den Abschnitten 1.3.1 bis 1.3.3 erläutert und dargestellt:

A. Konsistente Darstellung der Systemarchitektur und des Systementwicklungsprozesses inklusive Schnittstellen zur Integration in ETCS und anderen Zugbeeinflussungssystemen
B. Erarbeitung einer Methodik zu Nachweisführung und Begutachtung für außerhalb des Schienenverkehrs entwickelte Komponenten
C. Nachweis der sicheren Funktionalität der Ortungseinheit

1.3.1 Teilziel A: Konsistente Darstellung der Systemarchitektur

Die Systemarchitektur soll auf den relevanten terminologischen Grundlagen aufbauen, um die Definition des Systems und dessen Entwicklungsprozess konsistent darstellen zu können. Dafür sind zunächst die zu erfüllenden Anforderungen strukturiert darzustellen. Auf Grundlage dessen können die Spezifikationen und darauf aufbauend die strukturierte Gliederung des Systems während einer sicherheitsgerichteten Systementwicklung erstellt werden. Wenn bestehende Verfahren und Werkzeuge nicht genutzt werden können, ist deren Neuentwicklung zu forcieren.

Bestandteil der Systemarchitektur ist die Abgrenzung zu Komponenten, die nicht Teil des Systems sind. So soll die Kommunikation der Ortungseinheit durch die fahrzeugseitige Schnittstelle des spezifischen Übertragungsmoduls (Specific Transmission Module – STM) zum Stellwerk hier nicht betrachtet werden, die Kommunikation zwischen den Komponenten hingegen schon. Betrachtet werden hierfür zu definierende interne Kommunikationsschnittstellen. Die externe Kommunikation des Zuges aus sollte nur mit einer Schnittstelle abgewickelt werden. Diese ist einheitlich zu definieren, um einen interoperablen Schienenverkehr entsprechend den TSI [EU/2012/88] zu gewährleisten, womit die Kompatibilität zu ETCS ermöglicht wird.

1.3.2 Teilziel B: Sicherheitsgerichteter Entwicklungsprozess

Die sicherheitsrelevante Nutzung der satellitenbasierten Ortung im Schienenverkehr ergibt die Herausforderung, den Sicherheitsnachweis im bestehenden normativen Rahmen unter innovativen Randbedingungen durchzuführen. Dies soll durch die Erarbeitung einer Methodik zur generischen Nachweisführung im Schienenverkehr gewährleistet werden.

Die Analyse des normativen Rahmens, welcher eine Grundlage für die Entwicklung und den Nachweis der Sicherheit ist, fokussiert sich auf den primären Einsatzbereich der satellitenbasierten Ortungseinheit, Europa. Um eine weltweite Einsetzbarkeit zu ermöglichen, wird ein internationaler Bezug hergestellt. In Europa ist dabei der sich ändernde rechtliche Rahmen zu berücksichtigen, durch den sich ein Wandel der Verantwortlichkeiten von den Behörden, die durch die Gesetzgebung der Nationalstaaten festgelegt sind, zu den Behörden welche durch die europäische Gesetzgebung vorgegeben sind, vollzieht.

Das Aufzeigen der notwendigen Schritte zur Durchführung der Nachweisführung ist ein Alleinstellungsmerkmal dieser Arbeit, da diese noch nicht durchgeführt wurde. Es wird ein generischer Ansatz zur Durchführung des Sicherheitsnachweises auf Basis der gültigen Normung und vorangegangener Projekte vorgeschlagen. Mit diesem generischen Sicherheitsnachweis wird eine bedeutende Grundlage für die Zertifizierung der satellitenbasierten Ortung im Schienenverkehr durch nationale und europäische Behörden gelegt. Die dafür notwendige Entwicklung wird dabei als Prozesskette, die sich aus dem normativen Rahmen und weiteren zu berücksichtigenden Randbedingungen, bspw. seitens des Herstellers oder des potentiellen Betreibers ergibt, betrachtet. Zusätzlich zu Sicherheitsaspekten ist auch die Haftung während der Entwicklung und beim späteren Betrieb der Ortungseinheit von Bedeutung, sie wird jedoch in dieser Arbeit nicht im Detail betrachtet.

1.3.3 Teilziel C: Nachweis der sicheren Funktionalität

Die sichere Funktionalität der satellitenbasierten Ortungseinheit wird durch die Sensoren und deren Auswertealgorithmen ermöglicht. Qualifizierte Ortungsinformationen werden in Echtzeit geliefert, um die Sicherheits- und Genauigkeitsanforderungen des Schienenverkehrs kontinuierlich zu erfüllen. Dafür sind Anforderungen an Dokumente, Prozesse, Informationen und Randbedingungen für den jeweiligen Einsatzbereich zu definieren und darzustellen. Als Teil dessen sind Sicherheitsziele zu definieren und zu allokieren. Dabei ist sich den Herausforderungen der Entwicklung innovativer Leit- und

Sicherungssysteme mit übersichtlichen Verfahren und unterstützenden Werkzeugen zu stellen.

Für eine Gliederung der jeweiligen Einsatzbereiche werden die im Schienenverkehr möglichen Anwendungen der GNSS entsprechend ihrer sicherheitskritischen und rechtlichen Relevanz mit einer eingeführten Methodik strukturiert. Durch den erstmaligen Einsatz von nicht nach Sicherheitsvorgaben des Schienenverkehrs entwickelten industriellen Komponenten (Components Off The Shelf – COTS) wie GNSS-Empfänger und Wirbelstromsensor sind besondere Schritte durchzuführen, welche in dieser Arbeit analysiert und durchgeführt werden.

Für die Anwendung der satellitenbasierten Ortungseinheit und deren sichere Funktionalität sind auch die betrieblichen Rahmenbedingungen zu beachten. Aufgrund nationaler Betriebsordnungen ist eine Implementierung von sowohl ETCS als auch der satellitenbasierten Ortungseinheit nur durch Kooperation von EVU und EIU möglich.

1.4 Struktur dieser Arbeit

Der strukturierte Aufbau dieser Arbeit ermöglicht die konsistente Umsetzung der gestellten Ziele mit dem Ergebnis eines Vorschlags zur Sicherheitsnachweisführung im Schienenverkehr unter Nutzung von COTS am Beispiel der satellitenbasierten Ortung.

Dafür werden nach diesem einleitenden Kapitel in Kapitel 2 der Stand der Forschung und Technik und in Kapitel 3 der normative Rahmen dieser Arbeit dargestellt, um dem Leser kurz, aber trotzdem in der notwendigen Ausführlichkeit das Verständnis des Vorgehens und der Ergebnisse zu ermöglichen. In Kapitel 4 wird die strukturierte Beschreibung eines technischen Systems und dessen Entwicklung eingeführt, womit Teilziel A, eine konsistente Darstellung einer Systemarchitektur, erreicht wird. Aufbauend auf Stand der Technik und normativen Rahmenbedingungen wird der sicherheitsgerichtete Entwicklungsprozess entwickelt und dargestellt, womit Teilziel B (sicherheitsgerichtete Entwicklung) vollständig erreicht wird und für Teilziel C (sichere Funktionalität) die Grundlage gelegt wird. In den Kapiteln 5, 6, 7 und 8 wird als Kern dieser Arbeit der Entwicklungsprozess zur Nachweiskonzeption und -führung angewandt, womit Teilziel C komplettiert wird. Die beschriebene Struktur ist in Abbildung 1-2 dargestellt. Die in dieser Arbeit vorgenommene Verknüpfung der Systeme satellitenbasierte Ortung und Schienenverkehr ermöglicht eine Nutzung der Ressourcen der satellitenbasierten Ortung im Schienenverkehr.

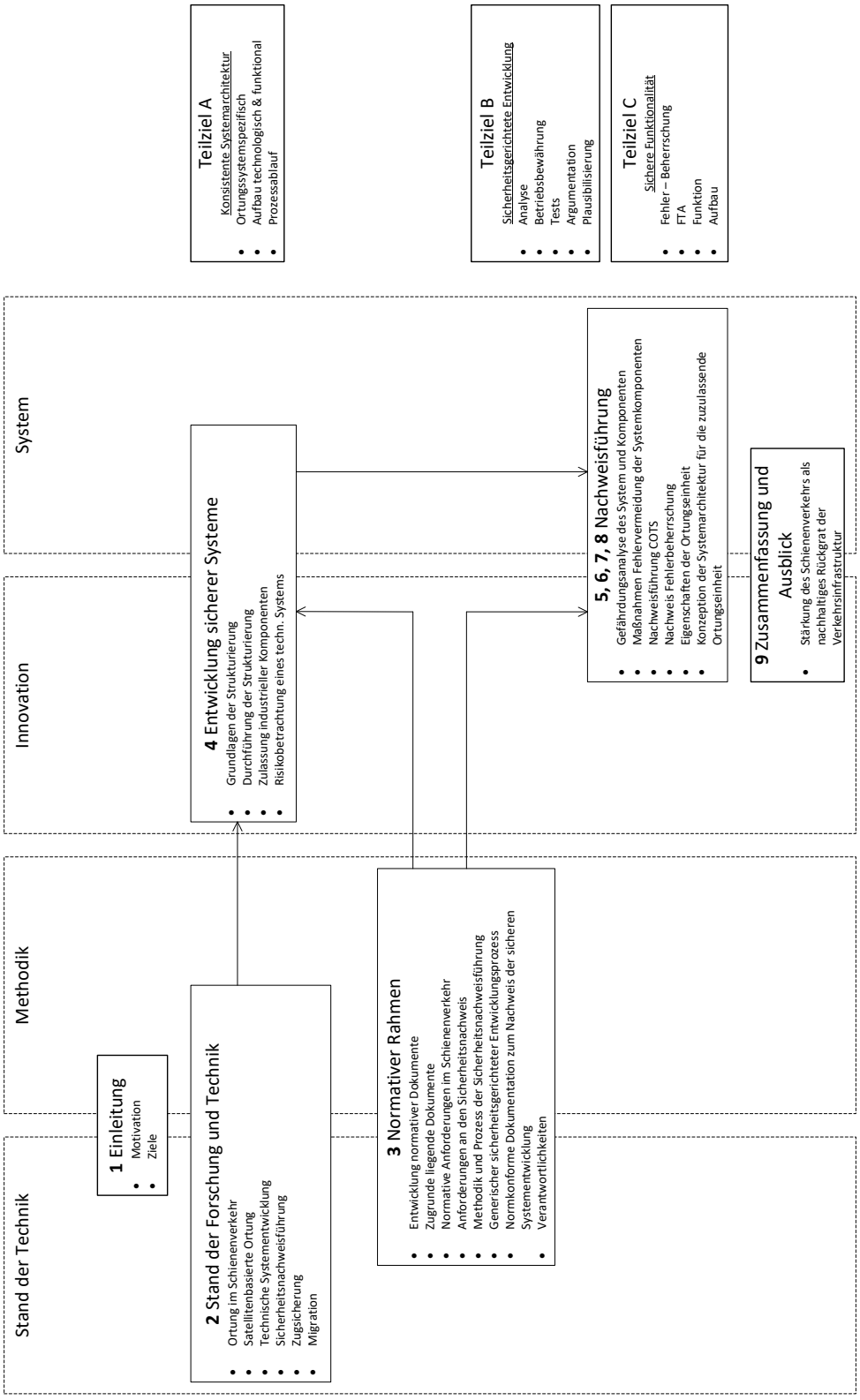


Abbildung 1-2: Struktur dieser Arbeit

2 Stand der Forschung und Technik in Zugbeeinflussung und Ortung

In diesem Kapitel wird der dieser Arbeit zugrunde liegende Stand der Forschung und Technik beschrieben. Zunächst werden in Abschnitt 2.1 Leitsysteme zur Steuerung des Verkehrssystems Eisenbahn betrachtet, für welche die satellitenbasierte Ortung als sichere Komponente genutzt werden soll. Dafür ist eine Migration notwendig, die dafür notwendigen Prozesse werden in Abschnitt 2.2 eingeführt.

Da diese Arbeit eine innovative Komponente zur Ortung von Schienenfahrzeugen einführt, wird der Stand der Technik dieses Themengebiets in Abschnitt 2.3 dargestellt. Darauf aufbauend wird in Abschnitt 2.4 die satellitenbasierte Sensorik für eine geplante, zukünftige Nutzung in der nötigen Detaillierung eingeführt. Zur effizienten Durchführung des Entwicklungsprozesses wird in Abschnitt 2.5 der Stand der Technik der Entwicklung technischer Systeme im Schienenverkehr dargestellt.

2.1 Leitsysteme zur Steuerung des Verkehrssystems Eisenbahn

Zum Verständnis der für diese Arbeit bedeutenden Leitsysteme des Schienenverkehrs werden in Abschnitt 2.1.1 Zugbeeinflussungssysteme allgemein eingeführt und darauf aufbauend in Abschnitt 2.1.2 eine Gliederung vorgeschlagen. Die derzeitige Anwendung von Zugbeeinflussungssystemen in Europa wird in Abschnitt 2.1.3 beschrieben. Dieser Status ist im Wandel, was in Abschnitt 2.1.4 betrachtet wird und zur in Abschnitt 2.1.5 beschriebenen Umsetzung führt. In Abschnitt 2.1.6 wird der derzeitige Stand der Technik der Nutzung von ETCS in Europa dargestellt.

2.1.1 Einführung Zugbeeinflussungssysteme

ZUGBEEINFLUSSUNGSSYSTEME[2] ermöglichen durch die Kenntnis der Position des Zuges Schutzfunktionen wie Sicherung der Weichen, Blocksicherung und Fahrstraßensicherung [Fenner et al. 2003; Maschek 2015]. Dabei wird das stete Ziel verfolgt, Unfälle im Schienenverkehr zu verhindern und ihre Folgen zu reduzieren.

> „Zugbeeinflussungsanlagen sind Anlagen, die Informationen über die zulässige Fahrweise vom Fahrweg zum Fahrzeug übertragen und bei Abweichungen von der zulässigen Fahrweise auf dem Fahrzeug entsprechende Schutzreaktionen (in der Regel Zwangsbremsungen) auslösen. Je nach

[2] In der Literatur werden „Zugsicherung“ und „Zugbeeinflussung“ teilweise unterschiedlich als Versuch der Unterscheidung, teilweise jedoch auch Synonym verwendet. Basierend auf Pachl [2013], wo ausschließlich "Zugbeeinflussung" genutzt wird, wird in dieser Arbeit auf die Nutzung von "Zugsicherung" verzichtet. Aufgrund der in dieser Arbeit verwendeten Termini wird anstatt der von Pachl [2013] vorgeschlagenen Benennung „Zugbeeinflussungsanlage“ „Zugbeeinflussungssystem“ genutzt.

> technischer Ausstattung wirken Zugbeeinflussungssysteme entweder nur als Ergänzung des ortsfesten Signalsystems oder ermöglichen eine Führung des Zuges nach Führerraumanzeigen unter Verzicht auf ortsfeste Signale.“ [Pachl 2013]

Nach [Meyer zu Hörste 2004] haben derartige Systeme, die dort als Eisenbahnleit- und Sicherungssystem (ELSS) bezeichnet werden, vergleichbare generische Funktionen, die auf der Klassifikation möglicher Gefährdungen und Funktionen basieren, bspw. die Sicherung der Fahrstraße oder die Überwachung der Geschwindigkeit. Zugbeeinflussungssysteme sollen dabei die Gefahr von Fehlern der Fahrer und damit das Risiko von Unfällen reduzieren bzw. eliminieren. Bei Eintreten von Fehlern soll eine sicherheitsgerichtete Reaktion, z. B. eine Zwangsbremsung bei Nichtbeachtung eines Signals, stattfinden. Der Begriff Zugbeeinflussung bezeichnet somit die fahrweg- und fahrzeugseitige Sicherung einer Zugfahrt, die entsprechende Regelungsfunktion kann durch Sicherungssysteme unterstützt werden [Schnieder 2007].

2.1.2 Gliederung der Zugbeeinflussungssysteme

Zugbeeinflussungssysteme lassen sich in diskrete und kontinuierliche Systeme gliedern. Diskrete Systeme nutzen zur Ortung elektronische Baken, die induktiv oder per Funk Informationen von der Strecke an den Zug übertragen oder codierte Gleisschaltkreise. Kontinuierliche Systeme übertragen permanent Daten und überwachen die Position des Zuges mit Hilfe elektrisch induktiver Kopplung, Gleisschleifen oder Funkübertragung zu jedem Zeitpunkt der Fahrt [Connor et al. 2014], was zukünftig durch GNSS realisiert werden soll.

Die Übertragung der Informationen zwischen fahrzeug- und streckenseitigen Komponenten kann berührungslos oder mit Kontakt erfolgen, wobei die Ortung dabei eng mit dem Zweck der Zugbeeinflussung verknüpft ist. Berührungslose Systeme wie PZB, LZB, Balise und RFID bestehen aus einer streckenseitigen Sendeantenne und einer fahrzeugseitigen Empfangsantenne. Achszähler und Gleisstromkreis sind lediglich an der Strecke installiert. Systeme, welche eine Berührung erfordern, sind selten, diese sind bspw. das französische System Crocodile oder in Deutschland der Weichensperrkreis [Pachl 2013].

2.1.3 Entwicklung und Anwendung der Zugbeeinflussung in Europa

Der technische Fortschritt von Zugbeeinflussungssystemen basiert unter anderem auf der Auswertung von Unfällen und dem Wunsch, dass ähnliche Fehler nicht erneut auftreten. Die Aufzeichnung erfolgt heutzutage durch Black Boxes, bei ETCS sind derartige Geräte

die JRU (Juridical Recording Unit). Damit wird die Überwachung durch zählpflichtige Bedienhandlungen im Fahrzeug oder Stellwerk ergänzt.

Heutige Zugbeeinflussungssysteme wurden nicht auf Grundlage erstellter Anforderungen konzipiert sondern basieren auf im 19. Jahrhundert entworfenen Konzepten [Thomas et al. 2008], die im 20. Jahrhundert als Reaktion auf Unfälle weiterentwickelt wurden. So wurde im Vereinigten Königreich das Zugbeeinflussungssystem AWS (Automatic Warning System) 1952 nach einem Unfall mit 112 Toten entwickelt, nach einem weiteren Unfall 1969 wurde es zur permanenten Geschwindigkeitsüberwachung erweitert. Ein erneuter Unfall 1975 führte zu einer Überwachung temporärer Geschwindigkeitsbeschränkungen [Connor et al. 2014].

Aufgrund ihrer national getrennten Entwicklung unterscheiden sich die verschiedenen europäischen Systeme meist signifikant voneinander. Aus dieser Vielfältigkeit resultieren Hindernisse für die von der EU geforderte Interoperabilität zwischen den Nationalstaaten Europas. Die Diversität wächst aufgrund des Einsatzes verschiedener Zugbeeinflussungssysteme auf verschiedenen Streckenkategorien in einem Land, so werden bspw. in den Niederlanden fünf Zugbeeinflussungssysteme parallel eingesetzt, zusätzlich existieren dort Strecken ohne Zugbeeinflussung [Ministerie van Infrastructuur en Milieu 2013]. Eine Übersicht über die wesentlichen in Europa eingesetzten Zugbeeinflussungssysteme ist mit Stand von 2004 in Abbildung 2-1 dargestellt.

Abbildung 2-1: Zugbeeinflussungssysteme in Europa nach [Meyer zu Hörste 2004]

2.1.4 Wandel zur europäischen Zugbeeinflussung

Speziell die in Abbildung 2-1 dargestellte Diversität an Zugbeeinflussungssystemen war eine entscheidende Motivation für die Entwicklung von ERTMS (European Rail Traffic Management System) [Winter 2009], welches sich zu einem Maßstab der Zugbeeinflussung entwickelt hat, der weltweit in 38 Ländern [Cramer 2012; Strandberg et al. 2013] angewandt wird. ERTMS besteht aus dem Zugbeeinflussungssystem ETCS, einem Kommunikationssystem (GSM-R) und dem Europäischen Zugmanagementsystem (European Train Management Layer – ETML) [VDV 2008]. Da der Schwerpunkt dieser Arbeit auf der Ortung für die Zugbeeinflussung liegt, wird im Folgenden ETCS fokussiert.

Die Forschung und Entwicklung für ETCS begann etwa 1990 und wurde 2000 mit einer einheitlichen Spezifikation abgeschlossen (SRS 2.0.0) [Stanley 2011], die Grundlage für erste kommerzielle Projekte und Pilotstrecken war. In der darauf folgenden Validierungsphase, die zwischen 2000 und 2004 den Beginn der ersten kommerziellen ETCS-Projekte in Italien und Spanien beinhaltete, wurden die Mehrdeutigkeiten in der Auslegung der technischen Vorgaben schrittweise erkannt und behoben [VDV 2008]. Mit den gesammelten Erfahrungen wurden die technischen Spezifikationen angepasst und auf europäischer Ebene gesetzlich festgelegt (SRS 2.3.0d) [Stanley 2011].

2.1.5 Technische Umsetzung von ETCS

ETCS wurde in fünf Leveln geplant, davon ermöglichen Level 1 bis 3 technische Interoperabilität [Meyer zu Hörste 2004; Stanley 2011]. In Level 1 erfolgt die Signalisierung ausschließlich über die Strecke, ab Level 2 sind keine streckenseitigen Signale mehr vorhanden. Die Ortung erfolgt dabei mit Hilfe von Balisen, die durch virtuelle Balisen ersetzt werden können, welche bei Überfahrt dieselbe Handlung auslösen wie eine im Gleisbett verlegte Balise. Bei Level 3 wird auf die streckenseitige Zugvollständigkeitsüberprüfung verzichtet.

Um eine breite Anwendung von ETCS zu ermöglichen, sollten die Komponenten von verschiedenen Unternehmen hergestellt werden können und deren Kombination möglich sein. Dazu sind einheitliche technische Spezifikationen ohne die Möglichkeit verschiedener Interpretationen notwendig. Um dies zu gewährleisten, werden die Spezifikationen [UNISIG 2012] fortlaufend auf Basis des aktuellen Entwicklungsstands angepasst und weiterentwickelt. Zudem ist deren Abwärtskompatibilität festgelegt [VDV 2008]. Aufgrund der Größe des mit ETCS auszurüstenden Netzes ist über einen langen Zeitraum mit Parallelbetrieb zu rechnen, wobei die verschiedenen Systeme über ein spezifisches Übertragungsmodul verbunden sind.

2.1.6 Nutzung von ETCS in Europa

In vielen Nationalstaaten Europas wird die Einführung von ETCS forciert, weil die bestehenden Zugbeeinflussungssysteme veraltet und ineffizient sind [Ministerie van Infrastructuur en Milieu 2013]. ETCS wird gegenwärtig schrittweise auf den TEN des Schienenverkehrs, welche 47 % des Schienennetzes der EU umfassen [EC 2013a; UIC 2013], eingeführt. So haben sich Belgien, Dänemark und die Schweiz für eine landesweite Einführung von ETCS um 2020 entschieden. Bspw. in der Schweiz wird ETCS explizit als Zugbeeinflussungssystem der Zukunft bezeichnet [Roth 2014], da es die Führerstandsignalisierung ermöglicht, die notwendig ist, um schneller als 160 km/h zu fahren. Da diese Funktion ab Level 2 implementiert ist, werden Strecken, auf denen schneller als 160 km/h gefahren werden soll oder wo ein Ersatz bzw. Neubau des Stellwerks notwendig ist, direkt zu Level 2 migriert [Roth 2014]. Alle anderen Strecken werden zur Herstellung der Interoperabilität unter Nutzung der bestehenden Stellwerke mit Level 1 ausgestattet. Daraus ergibt sich eine notwendige Migration von 600 Fahrzeugen verteilt auf 40 Typen. Die Migration zu Level 1 soll schweizweit bis 2017 abgeschlossen sein, bis 2025 soll das gesamte Netz mit Level 2 ausgerüstet sein [Roth 2014]. Um dies zu ermöglichen, sind einige Probleme, wie bspw. die Ausrüstung von Bahnübergängen, für die ETCS noch nicht spezifiziert ist, zu lösen.

Auch in anderen Ländern – bspw. Luxemburg und Österreich – sind die Erfahrungen mit ETCS positiv. In Österreich wurde bspw. im Oktober 2014 eine Fehlerrate von unter 1 % und lediglich 200 auf ETCS zurückzuführende Verspätungsminuten erfasst und als Erfolg gewertet [Pisek 2014], obwohl diese Fehlerrate nicht dem im Schienenverkehr geforderten Sicherheitslevel (SIL 4) entspricht. Die in Österreich mit Level 2 ausgestatteten Strecken verfügen über traditionelle Zugbeeinflussungssysteme als Rückfallebene, die deutsche Strecke von Halle/ Leipzig nach Erfurt (seit Ende 2015) und weiter Richtung Nürnberg (ab Ende 2017), wird ausschließlich mit ETCS Level 2 ausgerüstet [Beyer/Fußy 2014]. Norwegen, das Vereinigte Königreich und Schweden verfolgen das Ziel der landesweiten Ausstattung mit ETCS für 2035 bis 2040 [Ministerie van Infrastructuur en Milieu 2013]. In Deutschland, Frankreich und Spanien fokussiert sich die Migration auf internationale Güterverkehrs- und Hochgeschwindigkeitskorridore [Ministerie van Infrastructuur en Milieu 2013], um europäischen Interoperabilitätsanforderungen zu entsprechen. Aufgrund der aktuellen Planungen wird die Anzahl der mit ETCS ausgerüsteten Streckenkilometer permanent steigen. Stand 2015 sind 850 km mit Level 1 [Feltz 2014; Prengel/Stadlbauer 2015] und 438 km mit Level 2 [Roth 2014; Pisek 2014] ausgerüstet. Auf 829 km des Streckennetzes ist die Migration zu Level 2 geplant [ÖBB Infra 2014; Beyer/Fußy 2014; Steindl 2015]. Eine Übersicht der Strecken ist in Anhang 2 dargestellt.

2.2 Migrationsprozesse im Schienenverkehr

Der Wandel von einem bestehenden zu einem neuen technischen System erfolgt aufgrund erwarteter Vorteile bspw. hinsichtlich Sicherheit, Kapazität und Kosten und wird als Migration bezeichnet. Weitere motivierende Faktoren sind bspw. die Erweiterung von Funktionen oder politische Vorgaben [Obrenovic 2009]. Für die Migration sind zunächst die vier wesentlichen Phasen des V-Modells, also Anforderungsanalyse (Funktionalität, Verlässlichkeit, Wirtschaftlichkeit), Systementwurf (Sicherheit), Einführung (Migration) und Betrieb von Bedeutung [Bikker/Schroeder 2002]. Ausfälle oder Änderungen im Betrieb führen zum erneuten Systementwurf und somit zur erneuten Planung und Durchführung der Migration.

Aufgrund der sich ergebenden Komplexität kann die Migration nur systematisch gelöst werden. Somit bietet sich eine Planung in Teilschritten und Phasenmodellen, im Rahmen derer fortschrittbezogene Aufgaben nacheinander dargestellt werden, an [Lackhove 2013]. Ein reguliertes, in Prozessen definiertes Vorgehen ist für die Migration im Bereich der Zugbeeinflussung notwendig und sinnvoll [Obrenovic 2009].

Zur Darstellung der Migrationsprozesse im Schienenverkehr wird in Abschnitt 2.2.1 zunächst die Durchführung der Migration betrachtet, in Abschnitt 2.2.2 wird anschließend der Prozess der Migration dargestellt. Darauf aufbauend werden in Abschnitt 2.2.3 die Besonderheiten der Migration von Zugbeeinflussungssystemen analysiert. Abschließend wird in Abschnitt 2.2.4 der Stand der Technik der Migration bezüglich der Weiterentwicklung von einem ETCS Level zum nächsten dargestellt.

2.2.1 Durchführung der Migration

Für eine Migration ist eine intensive Abstimmung zwischen den beteiligten Institutionen notwendig. Die Nutzung von Rückfallebenen während oder nach der Migration ist zu untersuchen, um Unterbrechungen des Betriebsablaufs minimieren zu können, auch wenn diese generell als nachteilig betrachtet werden können, da es Kosten verursacht und den Betrieb behindert.

Zur Migration müssen die Anforderungen, Funktionen und Komponenten des Ursprungs- und des Zielsystems gegenüber gestellt werden, um die endgültige Migrationsstrategie erstellen zu können [Lackhove 2013]. Dabei muss das Rahmenkonzept des Zielsystems in einer einheitlichen Sprache klar definiert sein. Dies geschieht unter Berücksichtigung von Anforderungen aller beteiligten Institutionen sowie politischen, rechtlichen, technischen, betrieblichen und wirtschaftlichen Planungsvorgaben. Der optimale Prozess ist dabei im Schienenverkehr von der Topologie

des Netzes, dessen Länge und den zu nutzenden Fahrzeugen abhängig und wird durch verschiedene Migrationsstrategien unter Nutzung strategischer Spielräume gegenüber gestellt.

Die Migration kann linientreu oder fahrzeugorientiert erfolgen [Bikker/Schroeder 2002]. Bei einer linientreuen Migration können bestehende Fahrzeuge nachgerüstet, neue Fahrzeuge können entweder mit Neu- und Altsystem oder nur mit dem neuen System ausgerüstet werden. Bei einer fahrzeugorientierten Umrüstung wird die Strecke auf das neue System umgestellt, wenn alle Fahrzeuge auf das neue System umgestellt sind und auch streckenseitig das Ende des Lebenszyklus der dort verwendeten Komponenten erreicht ist. Bei einer geplanten Neuanschaffung von Fahrzeugen müssen diese nicht migriert sondern in das Netz eingeführt werden. Auch ist der parallele Betrieb von Zugbeeinflussungssystemen während einer längeren Migration möglich. Diese Variante wird in den Niederlanden angewandt, wo zunächst das rollende Material und anschließend die Infrastruktur ausgetauscht wird [Ministerie van Infrastructuur en Milieu 2013]. Zur Bewertung, welche Methode anzuwenden ist, bietet sich die Kapitalwertmethode an.

Die Migration soll vielfältige Verbesserungen erreichen, daher ist eine Koordination im Gesamtnetz notwendig, um die Auswirkungen auf den laufenden Betrieb so gering wie möglich zu halten. Dies kann durch eine relativ kurze Unterbrechung des laufenden Betriebs oder durch eine längere Migration während des laufenden Betriebs erfolgen. Die Migration im laufenden Betrieb hat den Vorteil, den Betrieb nicht zu unterbrechen, sie dauert jedoch länger und ist komplexer. Bei einer Unterbrechung des Betriebs werden in einem sehr kurzen Zeitraum, möglichst nachts oder am Wochenende, viele Arbeitsschritte gebündelt, was einen hohen Koordinations- und Planungsaufwand erfordert. Die Migration von größeren Projekten bedarf dabei spezieller Strategien, die in der Erstellung von Normen münden können [Lackhove 2013].

Generell ist die Einführung eines neuen Zugbeeinflussungssystems durch unterstützende administrative Maßnahmen mit geringerem Zeit- und Kostenaufwand möglich [Bikker/Schroeder 2002]. Diese können bspw. die staatliche Förderung der Fahrzeugausrüstung sein oder die Festschreibung von Netzzugangskriterien.

2.2.2 Prozess der Migration

In diesem Abschnitt wird ein Migrationsprozess zur Systemeinführung im Schienenverkehr nach [Obrenovic 2009] eingeführt und in Abbildung 2-2 dargestellt, der in Abschnitt 7.4.2 auf die zu entwickelnde Ortungseinheit angewandt wird.

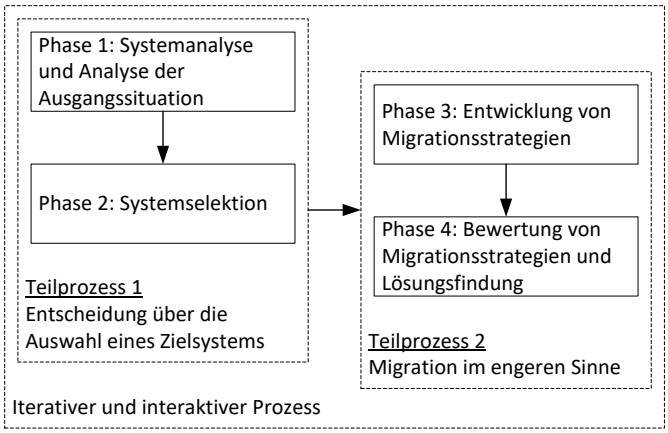


Abbildung 2-2: Migration im Schienenverkehr nach [Obrenovic 2009]

Der erste Teilprozess (Entscheidung über die Auswahl eines Zielsystems) gliedert sich in Phase 1 (Systemanalyse und Analyse der Ausgangssituation) und Phase 2 (Systemselektion). In Phase 1 wird das Zielsystem analysiert, das Systemumfeld geprüft und die Streckeneigenschaften betrachtet, damit die Maßnahmen spezifisch für die betrachtete Strecke getroffen werden können. Bei der Feststellung einer generellen Migrierbarkeit folgt Stufe 2. In Phase 2 werden notwendige technische Komponenten und Informationen vorbereitet. Aufbauend auf dem technischen Konzept ist die Umrüstung der Fahrzeuge konzeptionell festzulegen und ein Wartungs- und Instandhaltungskonzept zu entwickeln.

Der zweite Teilprozess (Migration im engeren Sinne) besteht aus Phase 3 (Entwicklung von Migrationsstrategien) und Phase 4 (Bewertung von Migrationsstrategien und Lösungsfindung). In Phase 3 werden mögliche Migrationsstrategien unter Beachtung relevanter Rahmenbedingungen und Einflussfaktoren für das ausgewählte technische System entwickelt. Der Hauptbestandteil ist dabei die physikalische Installation von Komponenten und deren Umrüstung im betrachteten System. Sämtliche Schritte dieser Stufe sind begleitet von sich iterativ wiederholenden Test- und Validierungsmaßnahmen. Die Phase schließt mit Nachweis der vollen Funktionsfähigkeit ab. Die Phase 4 betrifft die Bewertung von Migrationsstrategien sowie die Fertigstellung des Systems und dessen Übergabe an den Betreiber. Das Ergebnis des dargestellten Vorgehens ist ein integrationsfähiges technisches System mit einer optimierten, zugeschnittenen Migrationsstrategie [Obrenovic 2009].

2.2.3 Besonderheiten der Migration von Zugbeeinflussungssystemen

Durch die Komplexität und die Vielzahl an Beteiligten stellt eine Migration von Zugbeeinflussungssystemen eine Herausforderung dar. Sowohl der derzeitige Wandel zur europäischen Zugbeeinflussung ETCS als auch die Einführung der satellitenbasierten

Ortung im Schienenverkehr bedürfen einer Migration von einem Zugbeeinflussungssystem zum anderen [Gralla 2009]. Weiterhin wird auch die Migration innerhalb eines Zugbeeinflussungssystems zur Weiterentwicklung, bspw. von ETCS Level 1 zu ETCS Level 2, berücksichtigt. Bei einer Migration zu einem Level mit zusätzlichen Funktionen ergibt sich die Problematik der Kompatibilität der Systeme untereinander. Dem wird meist durch eine Abwärtskompatibilität begegnet, was jedoch zu eingeschränkten Funktionen des modernen Systems führen kann. Eine Herausforderung bei diesem Vorgehen ist die fehlende Erfahrung bei der Migration von Zugbeeinflussungssystemen in großen Netzen, lediglich Erfahrungen aus den Planungsprozessen in Dänemark, Belgien und der Schweiz können genutzt werden [Ministerie van Infrastructuur en Milieu 2013].

2.2.4 Migration zwischen verschiedenen ETCS Leveln

Als Basis für die Migration zwischen den ETCS Leveln wird das in Europa genutzte Level 2, wo die Ortung über Balisen und Hodometrie, die Zugvollständigkeitsprüfung und Gleisfreimeldung über Achszähler erfolgt, in (Abbildung 2-3) dargestellt [Hausmann/Enders 2007].

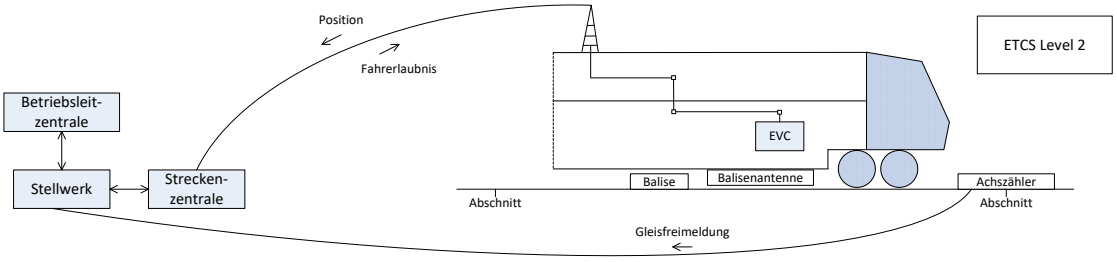


Abbildung 2-3: ETCS-Migration: ETCS Level 2

Die derzeitigen Planungen für ETCS Level 3 sehen die Zugvollständigkeitsprüfung zugseitig vor, weswegen eine streckenseitige Gleisfreimeldung durch Achszähler oder Gleisstromkreise nicht vorgesehen ist [Hausmann/Enders 2007]. Informationen über seine Position sollen dem Zug weiterhin über Balisen zur Verfügung gestellt werden, aktive Balisen ermöglichen die Übermittlung aktueller Informationen.

Als Anpassung an die derzeit bestehenden technischen Voraussetzungen wird hier ein reduziertes Level 3 eingeführt und als „ETCS Level 3-“ bezeichnet. Da derzeit keine technische Umsetzung für eine zugseitige Zugvollständigkeitsprüfung bekannt ist, wird diese dabei streckenseitig durchgeführt. Durch die Nutzung der satellitenbasierten Ortung kann auf die Übermittlung von Positionsinformationen durch die Balise verzichtet werden (Abbildung 2-4). Streckenseitig sind somit im Vergleich zu Level 2 keine

Migrationsschritte zu unternehmen, die verlegten Balisen werden nicht mehr genutzt. Die entsprechende Antenne am Zug kann abgebaut werden falls eine Nutzung des Fahrzeugs auf ETCS Level 2 Strecken ausgeschlossen werden kann. Lediglich eine Nachrüstung der Züge mit einer sicheren satellitenbasierten Ortung ist notwendig.

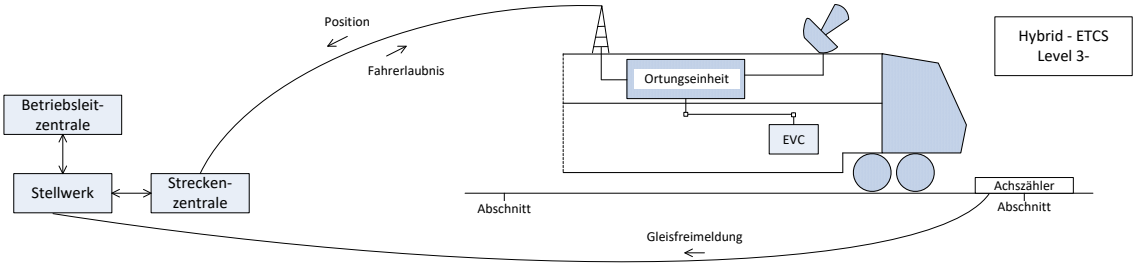


Abbildung 2-4: ETCS-Migration: ETCS Level 3-

Bei Lösung der Problematik der Zugvollständigkeitsprüfung oder auf Strecken im Inselbetrieb, auf denen diese auf andere Weise gewährleistet werden kann, ist eine Weiterentwicklung zu einem möglichen ETCS Level 4 ohne streckenseitige Einrichtungen möglich. Die Positionsbestimmung erfolgt über die satellitenbasierte Ortung, die Fahrerlaubnis wird über GSM-R übertragen (Abbildung 2-5).

Für diese möglichen ETCS Level ist die Entwicklung und Zertifizierung der sicheren satellitenbasierten Ortung für den Schienenverkehr notwendig.

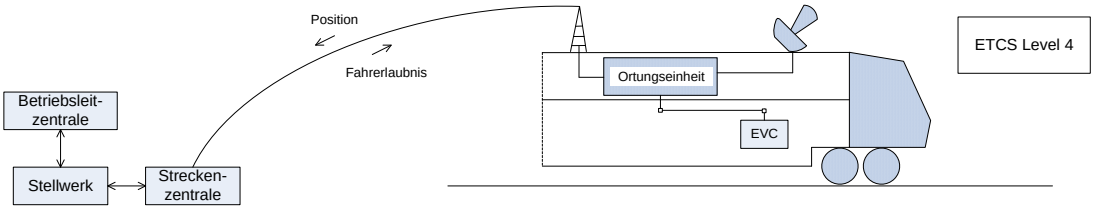


Abbildung 2-5: mögliches ETCS Level 4

2.3 Ortung im Schienenverkehr

Die ORTUNG im Schienenverkehr ist für dessen sichere Betriebsführung von großer Bedeutung. Flankenschutz, Folgefahrschutz und Gegenfahrschutz werden durch die Kenntnis der Fahrzeugposition ermöglicht, Schutz vor Entgleisungen durch Überwachung der Geschwindigkeit [Maschek 2015].

> „Ortung ist die Bestimmung des Bewegungszustands eines bestimmten Verkehrsmittels (d. h. Position, Geschwindigkeit nach Betrag und Richtung bezogen auf einen Bezugspunkt des Verkehrsmittels) in einem Bezugssystem.“ [Schnieder 2012]

Eine darauf aufbauende vertiefte Klassifikation von Ortungsmethoden wird in Abschnitt 2.3.1 vorgenommen. Auf die für diese Arbeit bedeutende kontinuierliche Ortung wird in Abschnitt 2.3.2 eingegangen. Um die für die Ortung notwendigen Informationen zu erhalten, sind Sensoren für die Datenaufnahme notwendig. Für die Verwendung in dieser Arbeit werden diese daher in Abschnitt 2.3.3 strukturiert und gegliedert. In Abschnitt 2.3.4 werden relevante fahrzeugseitige Sensoren eingeführt. Der derzeitige Stand der Nutzung von GNSS im Schienenverkehr wird in Abschnitt 2.3.5 betrachtet. In Abschnitt 2.3.6 werden in Betrieb befindliche, in Abschnitt 2.3.7 geplante satellitenbasierte Zugbeeinflussungssysteme vorgestellt.

2.3.1 Klassifikation von Ortungsmethoden

Die Ortung eines Objekts kann entsprechend verschiedener Methoden durchgeführt werden, deren Kombination mit Sensoren einen Einfluss auf das Sicherheitsniveau und die Durchführung des Betriebs hat [Kiriczi 1996; Leinhos 1996; Klinge 1998; Strang et al. 2008].

In [Klinge 1998] wird in Eigen- und Fremdortung, in [Leinhos 1996] in Nah- und Fernortung unterschieden. Die fahrzeugautarke Ortung ist dabei ein abgeleiteter Sonderfall der Eigenortung. Diese kann als Punktortung, Abschnittsortung, diskrete oder kontinuierliche Ortung beziehungsweise als relative oder absolute Ortung strukturiert werden [Leinhos 1996; Klinge 1998]. Für den weiteren Verlauf dieser Arbeit ist die Untergliederung in Eigen- und Fremdortung sowie in kontinuierliche und diskrete Ortung von Interesse.

Derzeit ist im Schienenverkehr eine Fremdortung üblich, die Fahrzeugposition wird hauptsächlich durch streckenseitige Sensoren bestimmt. Mit der Einführung der satellitenbasierten Ortung im Schienenverkehr ist ein Übergang zur Eigenortung des Fahrzeugs, welche auch als bordautonome Ortung bezeichnet wird [Strang et al. 2008], verbunden. Bei einer Fremdortung ist eine kontinuierliche Ortung nur mit sehr hohem Aufwand auf den entsprechend ausgerüsteten Abschnitten möglich, durch fahrzeugseitige Ortung ist diese jederzeit und überall im Netz realisierbar.

2.3.2 Fahrzeugseitige kontinuierliche Ortung

Die kontinuierliche Ortung kann zeitlich und räumlich aufgefasst werden und wird durch eine Echtzeitverarbeitung ermöglicht, jedoch wird diese unter anderem durch die Taktrate der einzelnen Sensoren, des verarbeitenden Rechners und der Datentransferrate des Bussystems begrenzt.

Eine kontinuierliche Ortung im Schienenverkehr lässt sich bspw. durch eine Positionsberechnung im Abstand von 200 ms erreichen, was bei einer auf Nebenstrecken maximal zulässigen Geschwindigkeit von 160 km/h eine Ortungsberechnung pro neun Meter gefahrener Strecke bedeuten würde. Dies ist zwar keine kontinuierliche Ortung im Sinne einer zu jedem Zeitpunkt zur Verfügung stehenden Ortungsinformation, jedoch durchaus kontinuierlich im Vergleich zur Länge der Streckenblöcke von 1.000 m oder mehr, zwischen denen die Position des Zuges dabei nicht bekannt ist. Im Projekt GaLoROI wurde bspw. eine Ortung im Abstand von fünf Sekunden als ausreichend betrachtet, um als kontinuierlich bezeichnet zu werden. Bei dieser Betrachtung wird deutlich, dass die exakten Anforderungen an die Ortung von den Anforderungen bezüglich Betrieb und Sicherheit der jeweiligen Strecke abhängig sind, sie sind somit schwer generisch zu betrachten. Aus den projektspezifischen Anforderungen an den maximalen Abstand zwischen zwei Ortungsinformationen lassen sich die Anforderungen an die Sensoren ableiten.

2.3.3 Strukturierung der zur Ortung verwendeten Sensoren

Sensoren werden zur Datenerfassung im Verkehr und somit auch zur Ortung genutzt. Sie machen sich dabei Wellenausbreitungseigenschaften bestimmter Signale zur Abstands- und/ oder Geschwindigkeitsmessung zunutze und verwenden verschiedene Auswerteverfahren wie Laufzeitmessung, Phasenmessung, Messung der Frequenzverschiebung (Ausnutzung des Dopplereffekts), Korrelation oder Triangulationsverfahren [Schnieder 2007].

Zur Ortung ist im Normalfall eine Kombination von Sensorsystemen notwendig, da für verkehrliche Anwendungen ein Sensor allein „nur in unzureichender Auflösung oder Unsicherheit (statisch, dynamisch) oder unzureichender Verlässlichkeit (Zuverlässigkeit, Instandhaltbarkeit, Verfügbarkeit und Sicherheit)“ [Schnieder 2007] Daten bereitstellen kann. Die Sensoren sind dabei an einer oder mehreren Verkehrskonstituenten (Verkehrsobjekt, Verkehrswegeinfrastruktur, Verkehrsorganisation und Verkehrsmittel [Schnieder 2007]) verortet und arbeiten selbstständig oder in Kombination von Sender und Empfänger. Die Verkehrsorganisation wird im Folgenden mit dem gängigeren Begriff Verkehrsleittechnik bezeichnet. Die Messgrößenerfassung kann dabei kontinuierlich, zeitdiskret oder ereignisdiskret erfolgen [Schnieder 2007].

Auf Grundlage der Kenntnis über das Wesen von Sensoren können diese gegliedert werden, was in Abbildung 2-6 entsprechend ihres Wirkprinzips und ihrer Verortung erfolgt. Dies ermöglicht im weiteren Verlauf dieser Arbeit aus den Anforderungen an die Sensoren die Spezifikationen abzuleiten, welche die Sensoren erfüllen müssen. Nach der

Analyse der Anforderungen der Anwendungen an die Ortungseinheit können Sensoren ausgewählt werden, welche die Anforderungen erfüllen.

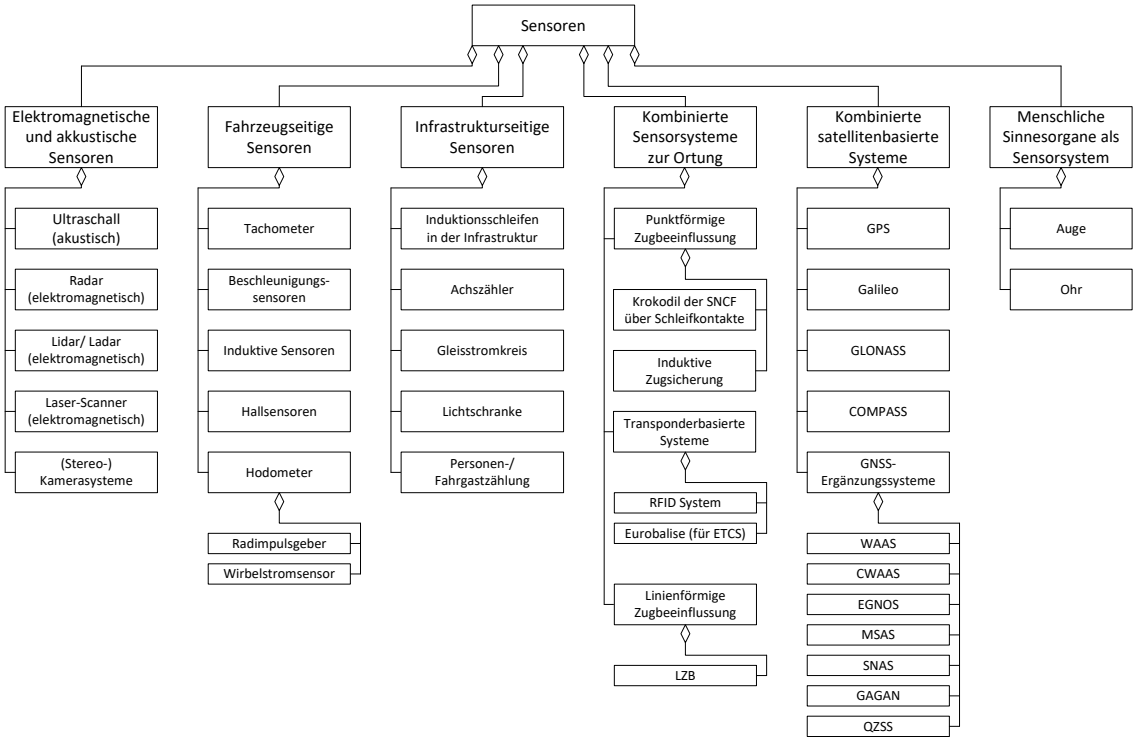


Abbildung 2-6: Gliederung von Sensoren nach [Schnieder 2007; Maschek 2015]

Die kombinierten Sensorsysteme nutzen fahrzeug- und infrastrukturseitige Sensoren, bspw. das Hodometer aus der Gruppe der fahrzeugseitigen Sensoren sowie Achszähler oder Gleisstromkreis als infrastrukturseitige Sensoren. Diese sind somit ein notwendiger Bestandteil der Ortung und Zugbeeinflussung. Sie bieten eine sichere und diskrete Ortung, jedoch verbunden mit hohen Wartungskosten [Marais et al. 2008].

2.3.4 Fahrzeugseitige Sensoren und digitale Karte

In diesem Abschnitt werden verschiedene fahrzeugseitige Sensoren und die digitale Karte eingeführt. Diese Sensoren sind der Inertialsensor, der Raddrehzahlgeber, der Radarsensor und der Wirbelstromsensor. Die Nutzung erfolgt insbesondere bei der Erstellung der Systemarchitektur in Abschnitt 7.1.2.1.

Der Inertialsensor ist im Inneren des Fahrzeugs montiert und ermittelt die Beschleunigung. Der Raddrehzahlgeber zählt durch den direkten Kontakt zwischen Fahrzeug und Infrastruktur die Umdrehungen des Rades, was jedoch mit Schlupf behaftet ist. Ein Radarsensor misst durch den Dopplereffekt elektromagnetischer Wellen die Bewegung des Fahrzeugs, die Geschwindigkeit, Strecke, Richtung und Beschleunigung. Der Einsatz ist bei Geschwindigkeiten bis 600 km/h möglich, Messungen auf

verschneiten Strecken sind jedoch fehlerbehaftet, Steinschlag kann weitere Probleme verursachen.

Der Wirbelstromsensor wurde als verlässlicher schlupffreier Sensor zur Wegstreckenmessung mittels magnetischer Interferenz für nicht sicherheitsrelevante Anwendungen im Schienenverkehr entwickelt [Engelberg 2001; Geistler 2007; Hasberg 2011; Hensel 2011], jedoch bisher nicht im Regelbetrieb eingesetzt. Zur Anwendung als Hodometer werden charakteristische Eigenschaften des Fahrzeugs, der Schiene und Weichen sowie weiterer Konstruktionsmaterialen [Schnieder et al. 2000] genutzt. Zudem kann die Fahrtrichtung bestimmt werden und an festen Wegmarken wie Weichen die exakte Position des Zuges bestimmt werden. Seine Eignung für eine verlässliche Nutzung im Fahrgastbetrieb wurde bei Tests in Deutschland und in der Slowakei in einem etwa einjährigen Test nachgewiesen [DemoOrt 2009].

Für jede Strecke, auf der ein Zug mit satellitenbasierter Ortung verkehren soll, ist eine digitale Karte notwendig. Diese kann alle Elemente der befahrenen Streckenabschnitte wie Länge der Geraden, Beginn und Ende der Bahnübergänge, Gefährdungspunkte, Weichenbereiche und Grenzzeichen, Gleisabschlüsse sowie Bahnhöfe darstellen. Ihre Leistungsfähigkeit wird durch eine permanente Aktualisierung und Verbesserung der Daten erhalten [Michler et al. 2013]. Als Grundlage für die Datenstrukturen bietet sich die Verwendung von Ergebnissen abgeschlossener Forschungsprojekte an [Georail 2008], so scheint die Nutzung von KML [ETSI 2012] und XML [McNeff 2012] als Sprachen sinnvoll. XML wird bereits in railML®, einer gebräuchlichen Darstellung für digitale Karten im Schienenverkehr, verwendet [railML 2013]. Zudem ist ein Echtzeitzugriff sinnvoll [Hasberg 2011]. Eine permanente Verbesserung der Karte gewährleistet eine hohe Qualität der Ortungsergebnisse.

2.3.5 Stand der Nutzung von GNSS im Schienenverkehr

Die Nutzung der satellitenbasierten Ortung im Schienenverkehr ist derzeit eingeschränkt, da eine Qualifikation der Ortungsinformation zur sicheren Anwendung notwendig ist. Wenn diese realisiert ist, können zusätzliche sicherheitsrelevante Anwendungen wie Bahnübergangssicherung, kostengünstige Zugbeeinflussung sowie Anwendungen für ETCS ermöglicht werden [Meyer zu Hörste et al. 2008]. Die Unterteilung der sicherheitsrelevanten Anwendungen von GNSS erfolgt im Folgenden in die Kategorien „in Betrieb befindliche“ (Abschnitt 2.3.6) und „geplante satellitenbasierte Zugbeeinflussungssysteme“ (Abschnitt 2.3.7). Aus diesen Anwendungen hat sich eine Standardsystemarchitektur der satellitenbasierten Ortungseinheit herauskristallisiert. Diese besteht aus den Sensoren GNSS-Empfänger, domänenspezifischem Hodometer,

digitaler Karte und einer Datenfusion in der Ortungseinheit und wird für die Erstellung der Systemarchitektur in Abschnitt 7.1.2 genutzt.

2.3.6 In Betrieb befindliche satellitenbasierte Zugbeeinflussungssysteme

Satellitenbasierte Zugbeeinflussungssysteme sind derzeit auf zwei Nebenstrecken in Österreich im Einsatz, die Implementierung in bestehende Systeme in Russland und den USA befindet sich in den Anfängen.

Das rechnergestützte Zugleitsystem (ZLB STH) wird in Österreich auf der 53 km langen Pinzgauer und auf einem etwa 100 km langen Streckennetz der Linzer Lokalbahn eingesetzt [Stadlmann 2007]. Die fahrzeugseitige Einrichtung besteht neben einer GPS Antenne aus einer Führerstandanzeige und einem Fahrzeugrechner. Der Fahrzeugrechner berechnet die Ortungsinformation aus GPS Daten und Eingaben des Triebfahrzeugführers, die Kommunikation erfolgt über ein dem Euroradio ähnliches Protokoll zum Fahrdienstleiter, der die Fahrerlaubnis erteilt. Die Ortung wird durch Rückfallweichen unterstützt. Bei Ausfall der satellitenbasierten Ortung wird Funkkommunikation als Rückfallebene genutzt [Stadlmann et al. 2012]. Das Grundkonzept des Systems wurde im Projekt SATLOC [Barbu 2012] um ein sicheres Kommunikationsnetzwerk erweitert und auf der 28 km langen rumänischen Strecke von Brașov nach Zărnești getestet.

In den USA sind Zugbeeinflussungssysteme, ebenso wie in Europa, untereinander nicht interoperabel, zudem ist auf 50 % der Strecken keine Zugbeeinflussungstechnik installiert, was in der Vergangenheit zu schweren Unfällen aufgrund menschlicher Fehler geführt hat [Petrek 2010]. Diese Problematik soll durch das inkrementelle Zugbeeinflussungssystem (Incremental Train Control System – ITCS) als Teil von PTC (Positive Train Control) [United States Congress 2008] gelöst werden, die Installation erfolgte aus finanziellen Gründen jedoch erst auf 66 Meilen des Netzes.

In Russland sind 30.000 Fahrzeuge mit dem modernen Zugbeeinflussungssystem Klub-U, welches die Möglichkeit der Geschwindigkeitsüberwachung und Zwangsbremsung bei Signalüberfahrt bietet, ausgerüstet. 12.000 Fahrzeuge davon sind mit Empfängern für GPS und GLONASS zur Unterstützung der Zugbeeinflussung ausgestattet [Shirres 2012]. Eine Erweiterung des Systems soll in Zusammenarbeit mit Ansaldo auf hochfrequentierten Strecken erfolgen und mit ERTMS kompatibel sein [Railway Insider 2010].

2.3.7 Konzepte satellitenbasierter Zugbeeinflussungssysteme

Im deutschen Projekt ALOIS wurde eine Echtzeitdatenerfassung und -übertragung für Disposition, Betriebsüberwachung, Befahrungsstatistiken und Kollisionsschutz [Koppers et al. 2000] durch die Ortung mit Empfänger für differentielles GPS, inertialem Richtungssensor und einem Hodometer bei optionaler Verwendung weiterer Sensoren verfolgt. Die Universität der Bundeswehr München und die Firma Tiefenbach GmbH verfolgten als Projektteilnehmer das Ziel, eine etwa 5.000 Euro teure Ortungseinheit zu entwickeln [Plan 2004]. Die Sicherheitsbetrachtung war nicht Teil des Projekts, die Praxistauglichkeit und korrekte Ortung wurde jedoch nachgewiesen.

Auch vom Institut für Verkehrssicherheit und Automatisierungstechnik der TU Braunschweig (iVA) wurden vielfältige Forschungstätigkeiten mit dem Ziel der Nutzung von GNSS im Schienenverkehr durchgeführt. Diese mündeten im gemeinsam mit der Deutschen Bahn (DB) durchgeführten Projekt SatZB [Meyer zu Hörste et al. 2001] und SATNAB [Däubler et al. 2002], wo die satellitenbasierte Ortung mit Hilfe petrinetzbasierter Modellierung auf Nebenstrecken als eigenständiges System genutzt werden sollte. Das Projekt konnte aufgrund fehlenden Interesses des EVU nicht mit einer betrieblichen Anwendung abgeschlossen werden. Die Zulassbarkeit wurde in GaLoROI nachgewiesen, der nächste Schritt ist die Serienfertigung [Becker/Manz 2016].

Das australische Advanced Train Management System (ATMS) soll die Kapazität der Strecken sowie die Verlässlichkeit und Sicherheit des Schienenverkehrs erhöhen, um die Infrastruktur- und Lebenszykluskosten signifikant zu reduzieren [Groves et al. 2010]. Für die mit ETCS Level 2 kompatible Positionsbestimmung sind dabei Gyroskop, Beschleunigungsmesser und digitale Karte geplant, was zu einer Genauigkeit von drei Metern führen soll. Nach abgeschlossenen Tests unter Laborbedingungen wird 2016 auf der Strecke zwischen Port Augusta und Whyalla ein Probebetrieb durchgeführt [ARTC 2015], die Gesamtkosten des Projekts werden auf 100 Mio. AU$ geschätzt [Hemsley 2014]. Nach erfolgreichem Abschluss der Tests ist 2017 ein Einsatz in weiten Teilen Australiens geplant, beginnend auf der Transaustralischen Eisenbahn zwischen Tarcoola und Kalgoorlie [Sadauskas 2015]. Bereits eingeführt wurde in Tasmanien das Advanced Network Control System (ANCS), welches Geschwindigkeiten, Positionen und die Belegung des Streckennetzes überwachen kann. Das System wurde mehrere Monate an der Nord-West Küste getestet und schließlich im ganzen Bundesstaat eingeführt [Sheridan 2015].

Der derzeit geringe Entwicklungsstand in vielen Ländern Afrikas eröffnet Potenziale für kreative und innovative Lösungen abseits von festgefahrenen Strukturen der Industrieländer und damit für eine dynamische wirtschaftliche Entwicklung. So ist in

Lagos, der größten Stadt Nigerias, ein schnelleres, günstigeres und verlässlicheres öffentliches Verkehrssystem geplant [The London Nigerian 2011]. Um dieses Ziel zu erreichen, hat das in Lagos ansässige Unternehmen Eko Rail 255 Züge aus Kanada gekauft, welche durch General Electric mit einem satellitenbasierten Zugbeeinflussungssystem ausgerüstet werden sollen, die Ortung erfolgt dabei mit GPS [The London Nigerian 2011].

Im noch laufenden Projekt 3InSat soll eine mit ERTMS kompatible satellitenbasierte Ortungsplattform für den Einsatz auf lokalen und regionalen Strecken mit niedrigem Verkehrsaufkommen sowie auf Güterverkehrsstrecken entwickelt und validiert werden [Berioli 2013]. Die erste Anwendung findet auf der 50 km langen Strecke von San Gavino Monreale nach Cagliari auf Sardinien statt, Ziel ist neben einer Steigerung der Kapazität und Effizienz die Zertifizierung mit dem Sicherheitsintegritätslevel (Safety Integrity Level – SIL) 4. Die Ortung wird durch eine lokale GNSS-Referenzstation ergänzt [Ansaldo STS 2014].

2.4 Satellitenbasierte Sensorik

Die für die Ortung notwendigen Informationen werden durch ein Ortungssystem zur Verfügung gestellt, dessen beispielhafte Ausprägungen in Abbildung 2-7 dargestellt sind. Dort senden die Satelliten des GNSS und die Balise als Beispiel für ein bakenbasiertes Ortungssystem Signale aus. Ein geodätisches Ortungssystem nutzt bestehende Landmerkmale mit Hilfe eines Theodolits als Sensor zur Ortung.

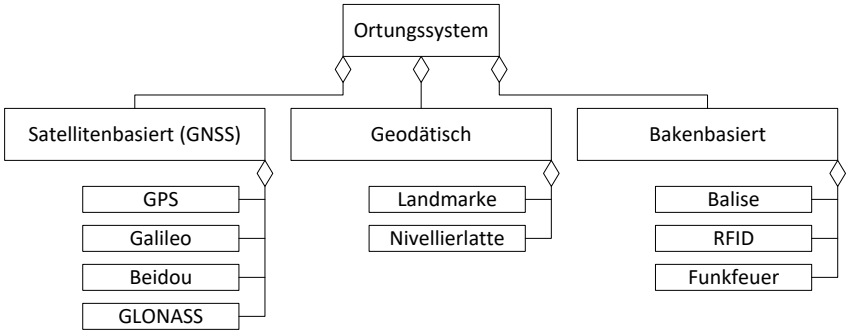


Abbildung 2-7: Ausprägungen und Komponenten eines Ortungssystems

In einer Ortungseinheit fließen die von einem oder mehreren Sensoren empfangenen Ortungsinformationen zusammen. Deren Architektur und die Anzahl der Sensoren richten sich dabei nach den Anforderungen an die Ortung im konkreten Anwendungsfall.

Als Grundlage für die Konzeption der satellitenbasierten Ortungseinheit wird in Abschnitt 2.4.1 die satellitenbasierte Ortung zunächst allgemein eingeführt, auf deren Funktionsweise und technische Aspekte wird in Abschnitt 2.4.2 eingegangen. Darauf

aufbauend werden in Abschnitt 2.4.3 die weltweit im Einsatz befindlichen GNSS dargestellt. Aufgrund des Fokus dieser Arbeit auf Europa wird in Abschnitt 2.4.4 das in Europa entwickelte GNSS Galileo mit seinen Besonderheiten und Diensten vorgestellt. In Abschnitt 2.4.5 werden Möglichkeiten zur Erhöhung der Genauigkeit betrachtet, in Abschnitt 2.4.6 werden dafür nutzbare Ergänzungssysteme eingeführt. Um Anregungen aus anderen Verkehrsdomänen für die Nutzung von GNSS im Schienenverkehr nutzen zu können, werden in Abschnitt 2.4.7 bekannte Anwendungen der satellitenbasierten Ortung in der Luftfahrt betrachtet.

2.4.1 Satellitenbasierte Ortung

Satellitenbasierte Ortung wird derzeit im Verkehr hauptsächlich für nicht sicherheitsrelevante Anwendungen, wie Verfolgung und Überwachung von Waren, Fahrgastinformationssysteme sowie Flottenmanagement, genutzt. Zukünftig ist die Nutzung für sicherheitsrelevante Anwendungen vorgesehen, wofür höhere Genauigkeiten und somit ausgereiftere Lösungen notwendig sind [Schnieder/Barbu 2009; Michler et al. 2013]. Damit sollen wirtschaftliche und betriebliche Vorteile erzielt werden, wofür eine Zertifizierung notwendig ist, deren Stand der Technik in Abschnitt 2.5 betrachtet und in den Kapiteln 5 bis 8 angewandt wird.

Die vier existierenden oder geplanten GNSS haben eine vergleichbare Funktionsweise, die in Abschnitt 2.4.2 dargestellt ist. Sie wird durch deren Ausprägungen und Komponenten, also Raumsegment, Bodensegment und Nutzersegment, die in Abbildung 2-8 dargestellt sind, ermöglicht.

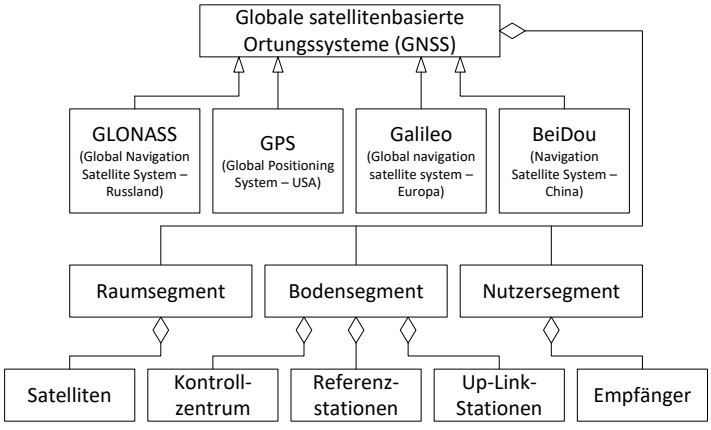


Abbildung 2-8: GNSS und ihre Ausprägungen sowie Komponenten

Das Raumsegment umfasst die Satelliten der GNSS und satellitenbasierter Ergänzungssysteme (Satellite Based Augmentation Systems – SBAS). Diese sind durch das Signal-In-Space mit dem Boden- und Nutzersegment verbunden. Im Nutzersegment

werden Empfänger zur Bestimmung der Position des Nutzers verwendet, im Bodensegment wird die korrekte Funktionalität der Satelliten überwacht und gegebenenfalls Korrekturdaten zu den Satelliten gesendet [Mansfeld 2009]. Das Bodensegment besteht aus Referenz- und Up-Link-Stationen sowie dem Kontrollzentrum. Damit kann die mögliche Abweichung der Genauigkeit der gesendeten Signale und die Bewegung der Satelliten auf deren Bahn überwacht und ggf. die Änderung ihrer Position veranlasst werden [Kaplan/Hegarty 2006; Bauer 2011].

2.4.2 Funktionsweise und technische Aspekte der GNSS

GNSS stellen ihren Nutzern in Ruhe und Bewegung „genaue Informationen über ihre (dreidimensionale) Position, ihre Geschwindigkeit sowie über die Zeit überall auf oder nahe der Erde zur Verfügung" [Bauer 2011]. Dafür stellen alle GNSS unabhängig der äußeren Bedingungen die geforderten Informationen – Position, Navigation und Zeit [Hofmann-Wellenhof et al. 2008; Mansfeld 2009] – ständig und zuverlässig zur Verfügung [Bauer 2011]. Diese Zusammenhänge und die dafür notwendige Kommunikation ist in Abbildung 2-9 dargestellt. Das Raumsegment sendet seine Nachrichten über die Satelliten aus, diese werden im Nutzersegment zur Positionsbestimmung und im Bodensegment zur Kontrolle des Status und der Richtigkeit der gesendeten Informationen empfangen und entsprechend verarbeitet.

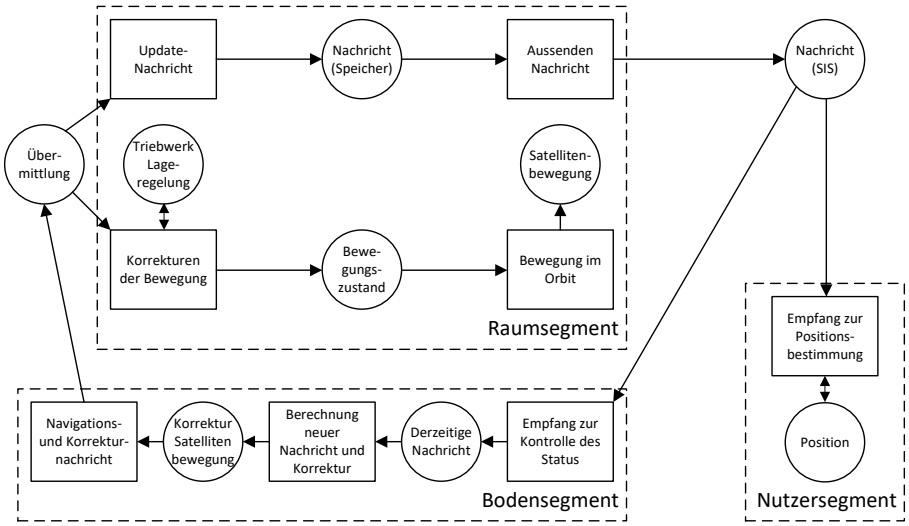


Abbildung 2-9: Segmente von GNSS nach [Schnieder et al. 2009a; Poliak 2009]

Zur Berechnung der Ortungsinformation im Nutzersegment müssen jederzeit an jedem Punkt der Erde mindestens vier Satelliten sichtbar sein [Dodel/Häupler 2009], woraus sich die Anzahl der Satelliten im Weltraumsegment der einzelnen GNSS, welche in Tabelle 2-1 dargestellt sind, ergeben. Daneben haben auch Bahnhöhe und -neigung Einfluss auf die Ortungsqualität.

Tabelle 2-1: Systemparameter (Sollwerte der realisierten und geplanten GNSS) [Bauer 2011]

Systemparameter	GPS (USA)	GLONASS (Russland)	Galileo (Europa)	Beidou (China)
Anzahl der Satelliten	24	24	27	27
Bahnebenen	6	3	3	3
Bahnneigungen [Grad]	55	64,8	56	55
Bahnhöhe [km]	26.560	25.508	29.601	27.480

Höhere Bahnhöhen haben den Vorteil, dass weniger Satelliten für eine ausreichende Abdeckung der Erde benötigt werden, es erhöhen sich jedoch der Weg, den das Signal vom Satelliten zum Nutzer zurücklegen muss und somit die möglichen Fehlerquellen. Zudem erhöht sich der Aufwand, um die Satelliten ins Weltall zu bringen.

2.4.3 Weltweite GNSS

Von den in Abbildung 2-8 eingeführten GNSS können die militärisch entwickelten und betriebenen GPS (USA) und GLONASS (Russland) verwendet werden. GPS steht dabei seit etwa 1990 der zivilen Nutzung zur Verfügung [Kaplan/Hegarty 2006], GLONASS seit 2011 [Gibbons et al. 2013]. Das vom chinesischen Militär entwickelte Beidou befindet sich, genau wie das europäische Galileo, welches das einzige zivile System ist, im Aufbau.

Die bestehenden und in Entwicklung befindlichen GNSS haben sich durch verschiedene Dienste auf die Anforderungen der Nutzer eingestellt. Bspw. beim US-amerikanischen GPS bietet der zivile Dienst keinerlei Garantien, der militärische Dienst mit entsprechenden Zugangsbeschränkungen bietet hingegen Genauigkeitsgarantien [US Government 2012]. Mit einer etwa 2021 geplanten Einführung des L5-Bands sollen auch zivilen Nutzern garantierte Genauigkeiten und Verfügbarkeiten zur Verfügung stehen [NOAA 2014]. In Abbildung 2-10 ist ein Überblick über die Anzahl der für die GNSS in Betrieb befindlichen Satelliten mit entsprechender Prognose dargestellt.

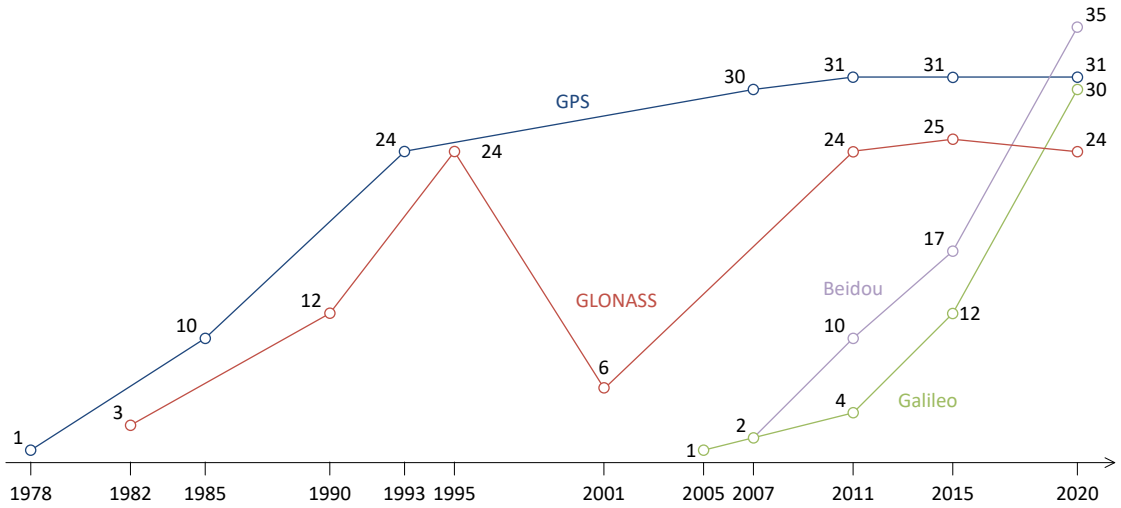


Abbildung 2-10: Aktuelle und prognostizierte Anzahl der betriebsfähigen Satelliten im Weltall [Federal Space Agency 2016; US Government 2016; GSC 2016; China National Space Administration 2016]

2.4.4 Galileo

Die zivile Ausrichtung von Galileo soll eine ununterbrochene GNSS-Versorgung als strategischen Vorteil für Europa sicherstellen und somit einen hohen Nutzen für die Bevölkerung herstellen [EC/ESA 2002]. Aufgrund von Verzögerungen in der Vergangenheit sind derzeit weniger Satelliten in Betrieb als geplant, Galileo scheint daher das letzte GNSS zu werden, welches seinen Nutzern eine volle Einsatzbereitschaft bietet. Nach aktuellem Kenntnisstand ist diese für 2019 geplant [Nurmi 2015]. Da sich andere GNSS auch weiterentwickeln, ist der zusätzliche Nutzen von Galileo derzeit schwer abschätzbar. In Einklang mit einer verbesserten Ortung sollen Innovationen durch neue Dienste, Ideen und Lösungen ermöglicht werden [Hernández et al. 2015].

Um die Anforderungen verschiedener Anwendungen – auch mit Sicherheitsbezug – zu berücksichtigen, wurden bei Galileo und dem europäischen Erweiterungssystem zur satellitenbasierten Ortung (European Geostationary Navigation Overlay Service – EGNOS), welches in Abschnitt 2.4.6 zusammen mit anderen weltweiten Ergänzungssystemen betrachtet wird, bereits in der Entwicklungsphase fünf verschiedene Dienste eingeplant. Für diese Arbeit relevant ist der sichere Dienst, der die garantierten Eigenschaften Integrität, Verfügbarkeit, Genauigkeit und Kontinuität bietet [EC/ESA 2002; Marais et al. 2008]. Gemäß der Definition der Internationalen Zivilluftfahrtorganisation (International Civil Aviation Organisation – ICAO), auf welcher die Entwicklung von EGNOS und Galileo aufbaut, bezieht sich die Genauigkeit auf die absolute horizontale Genauigkeit im 2σ-Konfidenzintervall von 95 %. Integrität beschreibt die Wahrscheinlichkeit, dass das System bestimmungsgemäß arbeitet und

beinhaltet das Integritätsrisiko, die Alarmzeit und das Alarmlimit. Alarmzeit beschreibt die Zeit, die das System benötigt, um den Nutzer vor seiner Nichtfunktion zu warnen. Kontinuität beschreibt die Fähigkeit des Systems, seine Funktion ohne ungeplante Unterbrechungen zur Verfügung zu stellen. Die Verfügbarkeit eines Dienstes beschreibt den unterbrechungsfreien Betrieb eines Systems mit der geforderten Genauigkeit, Integrität und Kontinuität [EC/ESA 2002; ICAO 2005; Shin et al. 2008]. Derzeit wird der sichere Dienst zu einem weniger leistungsstarken Dienst neu definiert [Hernández et al. 2015]. Dieser ist am besten für sicherheitsrelevante Anwendungen geeignet, da er spezifizierte Genauigkeits- und Integritätsinformationen anbieten soll.

Eine mögliche zukünftige Entwicklung ist, dass der kommerzielle Dienst anstatt des sicheren Dienstes zum genauesten und sichersten weltweiten Ortungsdienst ausgebaut wird. Somit hätte der kommerzielle Dienst die Aufgabe, eine im Vergleich zu anderen GNSS höhere Datenrate zu liefern und zu gewährleisten, dass die Datenübertragung innerhalb weniger Sekunden erfolgt und Integritätsinformationen in Echtzeit weltweit zur Verfügung stehen [Hernández et al. 2015]. Der kommerzielle Dienst soll eine hohe Genauigkeit im Zentimeterbereich liefern, bei einem Test wurde bereits eine Genauigkeit im Dezimeterbereich erreicht [Hernández et al. 2015].

2.4.5 Erhöhung der Genauigkeit

Die Dienste der derzeit in Betrieb befindlichen GNSS bieten lediglich für nicht sicherheitsrelevante Anwendungen eine ausreichende Genauigkeit; ob sie für die geplanten Dienste ausreicht ist noch nicht abschätzbar. Für sicherheitsrelevante Anwendungen sind daher Ergänzungssysteme zur Verbesserung der Genauigkeit und Verlässlichkeit der Ortung notwendig. Dies kann der in der Geodäsie genutzte zivile Internationale GNSS Service (IGS) sein, der entsprechende Daten liefert [Bauer 2011]. Die zugrunde liegenden Daten werden von sieben Analysezentren in Europa und Nordamerika durch einen Vergleich mit Referenzdaten bereitgestellt, die entsprechenden Systemparameter sind in Tabelle 2-2 dargestellt.

Tabelle 2-2: IGS GPS-Produkte [Bauer 2011]

Produkt		Ultra-Rapid (vorausberechnet)	Ultra-Rapid (beobachtet)	Rapid	Final
Verfügbarkeit		Echtzeit	3 Std.	17 Std.	13 Tage
Genauigkeit	Orbit	10 cm	5 cm	< 5 cm	< 5 cm
	Uhr	< 5 ns	~ 0,2 ns	0,1 ns	< 0,1 ns
Intervall	Orbit	15 min	15 min	15 min	15 min
	Uhr			5 min	5 min/30 s

Zur Nutzung dieser Daten ist eine Kommunikationsverbindung notwendig. Um nicht diese separate Schnittstelle aufbauen zu müssen, erscheint eine Übertragung von

Korrekturdaten via Satellit sinnvoll, was von SBAS realisiert wird, die im folgenden Abschnitt eingeführt werden.

2.4.6 Weltweite Ergänzungssysteme

SBAS nutzen geostationäre Satelliten zur Verbesserung der Genauigkeit von GNSS. In Abbildung 2-11 ist eine Übersicht über die weltweit existierenden SBAS, deren Ausprägungen und Einsatzgebiete dargestellt. Die dafür genutzten geostationären Satelliten bewegen sich in etwa 36.000 km Höhe synchron mit der Erde. Durch die große Höhe sind sie auf nahezu der halben Erdkugel sichtbar.

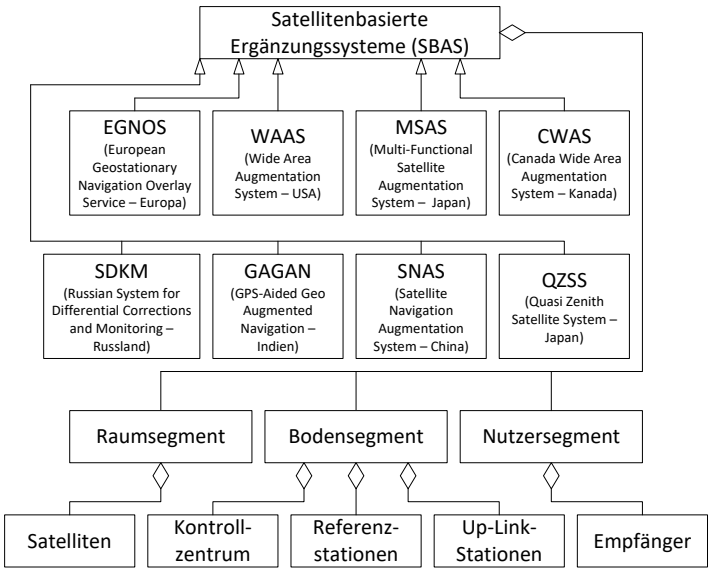


Abbildung 2-11: SBAS und ihre Ausprägungen

2.4.7 Anwendungen der Luftfahrt

Die Anwendung von GNSS in der Luftfahrt ist nicht originärer Bestandteil dieser Arbeit, mit Hilfe dieses Exkurses soll jedoch festgestellt werden, ob für den Schienenverkehr verwendbare Ansätze existieren, andernfalls sind neue Wege zu entwickeln.

Die Anwendung von GNSS in der Luftfahrt hat das Ziel, dass Strecken ohne Umwege durch Navigationspunkte geflogen werden können und Kapazität sowie Sicherheit erhöht werden. Zudem kann durch die Nutzung der satellitenbasierten Ortung zur Navigation die Ausrüstung und somit das Flugzeuggewicht reduziert werden. Erste Zertifizierungen von Flugzeugen und Flughäfen für Landeanflüge erfolgten am Flughafen Pau-Pyrenäen in Südfrankreich [GPS World 2011]. Auch die Zertifizierung vom indischen GAGAN für die Luftfahrt ist geplant; das auf 0,1 nautische Meilen genaue Abfliegen von Luftstraßen

und Landeanflüge mit geringen Genauigkeitsanforderungen (Nichtpräzisionsanflüge) ist bereits zertifiziert [Gibbons 2014]. Zudem existieren Empfehlungen bezüglich der betrieblichen Mindestanforderungen an GPS [DO 208], SBAS [DO 229D] und GBAS [DO 253C].

In der Luftfahrt werden die Anforderungen an GNSS, welche SBAS und/ oder GBAS nutzen, entsprechend typischer Betriebszustände gegliedert. Im Reiseflug wird lediglich eine Genauigkeit von 3,7 km und eine Alarmzeit von fünf Minuten gefordert, während Präzisionsanflügen ist eine Genauigkeit von 16 Metern und eine Alarmzeit von 6 Sekunden notwendig [ICAO 2004]. Weitere Anforderungen werden in den Kategorien vertikale Genauigkeit, Integrität, Kontinuität und Verfügbarkeit gestellt. Die jeweils geforderte horizontale und vertikale Genauigkeit ist dabei lediglich in 95 % der Fälle einzuhalten. Die Anforderungen entsprechend den Betriebszuständen sind in Tabelle 2-3 zusammenfassend dargestellt.

Tabelle 2-3: Anforderungen der Luftfahrt an GNSS [ICAO 2004]

Betriebszustand	Horizontale Genauigkeit 95 %	Vertikale Genauigkeit 95 %	Integrität	Alarm-zeit	Kontinuität	Verfügbarkeit
Reiseflug	3,7 km	N/A	$1\text{-}1x10^{-7}$/h	5 min	$1\text{-}1x10^{-4}$/h bis $1\text{-}1x10^{-8}$/h	$1\text{-}1x10^{-2}$ bis $1\text{-}1x10^{-5}$
Reiseflug im Flughafenbereich	0,74 km	N/A	$1\text{-}1x10^{-7}$/h	15 s	$1\text{-}1x10^{-4}$/h bis $1\text{-}1x10^{-8}$/h	$1\text{-}1x10^{-2}$ bis $1\text{-}1x10^{-5}$
Nichtpräzisions-anflug (NPA), Abflug	220 m	N/A	$1\text{-}1x10^{-7}$/h	10 s	$1\text{-}1x10^{-4}$/h bis $1\text{-}1x10^{-8}$/h	$1\text{-}1x10^{-2}$ bis $1\text{-}1x10^{-5}$
Anflug mit vertikaler Führung (APV-I)	16 m	20 m	$1\text{-}2x10^{-7}$/h pro Anflug	10 s	$1\text{-}8x10^{-6}$ in 150s	$1\text{-}1x10^{-2}$ bis $1\text{-}1x10^{-5}$
Anflug mit vertikaler Führung (APV-II)	16 m	8 m	$1\text{-}2x10^{-7}$/h pro Anflug	6 s	$1\text{-}8x10^{-6}$ in 150s	$1\text{-}1x10^{-2}$ bis $1\text{-}1x10^{-5}$
Kategorie I Präzisionsanflüge	16 m	6 bis 4 m	$1\text{-}2x10^{-7}$/h pro Anflug	6 s	$1\text{-}8x10^{-6}$ in 150s	$1\text{-}1x10^{-2}$ bis $1\text{-}1x10^{-5}$

Dabei wird deutlich, dass die Anforderungen für den Reiseflug und für den Nichtpräzisionsanflug weit gefasst sind, für Präzisionsanflüge der Kategorie 1 wird angenommen, dass die entsprechend gestellten Bedingungen nicht durch GNSS, auch wenn sie durch SBAS und GBAS unterstützt werden, zu erfüllen sind [Kaplan/Hegarty 2006].

Der wesentliche Unterschied, der zwischen Anwendungen der satellitenbasierten Ortung im Schienenverkehr und in der Luftfahrt deutlich wird, ist dass der Schienenverkehr die Genauigkeiten, welche der Luftverkehr im Anflug stellt, während der gesamten Fahrt stellt. Dies bezieht sich insbesondere auf den Wert der Alarmzeit der Luftfahrt des Reisefluges, der im Schienenverkehr zu keinem Zeitpunkt des Betriebs akzeptabel ist. Damit sind derzeitige für die Luftfahrt entwickelte Lösungen nicht ohne Anpassungen im

Schienenverkehr einsetzbar, zudem sind Abschattungen und Mehrwegausbreitung zu beachten [Lu 2014]. Auf den Schienenverkehr übertragbar ist die Unterscheidung der Anforderungen an die Ortung entsprechend den Betriebszuständen; verschiedene Phasen der Fahrt oder betrieblichen Situationen erfordern unterschiedliche Genauigkeiten.

2.5 Integration und Zertifizierung der satellitenbasierten Ortung

Zur Nutzung der satellitenbasierten Ortung für sicherheitsrelevante Anwendungen ist in allen Verkehrsdomänen – Straßenverkehr, Schienenverkehr, Wasserverkehr und Luftverkehr – eine Zertifizierung nach domänenspezifischen Kriterien notwendig.

Die sichere Anwendung von Ortungssystemen im Verkehr bedingt, dass eine geforderte Genauigkeit und Verlässlichkeit der Position des betreffenden Objekts (Fahrzeug) nachgewiesen wird. Dies geschieht unter anderem über die attribuierbaren Merkmale wie Richtigkeit, Messunsicherheit sowie zeitliche und geographische Verfügbarkeit. Weiterhin müssen wirtschaftliche, organisatorische und rechtliche Eigenschaften sowie die Haftung im Fall eines möglichen Versagens des Systems betrachtet werden [Schnieder 2009]. Für den Nachweis der messbaren Größen muss eine Verifizierung der spezifizierten Messqualität entsprechend aller gängigen Normen durchgeführt werden. Der Nachweis der sicheren Nutzbarkeit erfolgt durch eine generische Zertifizierung des GNSS im Raum- und Bodensegments und eine domänenspezifische Zertifizierung der Ortungseinheit im Nutzersegment. Eine generische Zertifizierung des GNSS erfordert den Nachweis dessen Sicherheit und/ oder des entsprechenden SBAS.

Zum Nachweis der Genauigkeit ist eine technische Integration und darauf aufbauend die Zertifizierung der Ortungseinheit notwendig, in Abschnitt 2.5.1 wird der Stand der Technik der generischen Zertifizierung und in Abschnitt 2.5.2 der domänenspezifischen Zertifizierung von GNSS betrachtet. Da der Empfänger der satellitenbasierten Ortung als industrielle Komponente (COTS) in die Ortungseinheit integriert werden soll, wird in Abschnitt 2.5.3 die Zertifizierung von COTS fokussiert und darauf aufbauend Beispiele dargestellt, um dort gewonnene Erkenntnisse für diese Arbeit nutzen zu können.

2.5.1 Generische Zertifizierung satellitenbasierter Ortungssysteme

Eine generische Zertifizierung von GNSS oder SBAS ist spezifisch für das jeweilige System, also bspw. GPS oder Galileo, durchzuführen. Derzeit existieren lediglich für das zivile System Galileo Spezifikationen [EC/ESA 2002], anhand derer eine Zertifizierung möglich ist. Der seit März 2011 in Betrieb befindliche [GPS World 2011] sichere Dienst von EGNOS, dem Galileo zugeordneten SBAS, soll als einziger Dienst zertifizierte

Genauigkeiten bieten. Für GPS bestehen seit den 1990ern noch nicht realisierte politische und wirtschaftliche Forderungen zur Zertifizierung von Empfängern mit einem Test [McNeff 2012].

Eine generische Zertifizierung der GNSS für verschiedene Verkehrsdomänen wird derzeit nicht als realistisch erachtet, weil verschiedene Verkehrsdomänen unterschiedliche Einsatzprofile und Anforderungen haben und für die weitere Entwicklung der GNSS kein bezüglich derer Zertifizierung belastbarer Zeitplan vorliegt. Prinzipiell müsste die Zertifizierung separat für jeden Dienst von bspw. Galileo oder GPS durchgeführt werden.

Der Empfänger stellt dem Nutzer die Ortungsinformation zur Verfügung, weswegen dieser bei der Zertifizierung, welche Technik, Leistung und Sicherheit umfasst [McNeff 2012], im Fokus steht. Bei der technischen Zertifizierung des Empfängers muss nachgewiesen werden, dass dieser den Schnittstellenanforderungen entspricht. Die daran anschließende Zertifizierung beinhaltet den Nachweis der Präzision, Richtigkeit und Integrität der Navigationsnachricht sowie die Untersuchung, ob externe Korrekturen (SBAS/ GBAS) korrekt berücksichtigt werden. Bei der Sicherheitszertifizierung werden der Schutz vor unabsichtlicher und absichtlicher Störung der Signale und die Verschlüsselung betrachtet.

Zur Überprüfung der durch den Empfänger gelieferten Genauigkeit haben [Hänsel 2008] und [Wegener 2013] eine Methode zu deren Zertifizierung vorgeschlagen und weiterentwickelt. Laboratorien und Zertifizierungsstellen sollen eine Akkreditierung erhalten, Empfänger satellitenbasierter Ortungssysteme für eine bestimmte Genauigkeit zu zertifizieren. Dafür werden verschiedene Anforderungen an die statische und dynamische Messgenauigkeit und die Zeit bis zur ersten Positionsbestimmung (Time to first fix – TTFF) gestellt, die mit den Messergebnissen verglichen werden. Dieser Prozess soll zudem in einer Norm abgebildet werden [Hänsel 2008]. Aufbauend auf diesen Ergebnissen wurden Referenzmesssysteme erstellt, welche die Genauigkeit der satellitenbasierten Ortung eines sich bewegenden Empfängers ermittelten [DemoOrt 2009; Wegener et al. 2010]. Diese Arbeiten bildeten die Basis für Untersuchungen zur Qualität von Messergebnissen und zu Messabweichungen [Wegener 2013] und eine Methode zur Auswertung der Messergebnisse des Referenzmesssystems [Grasso Toro et al. 2012; Spiegel et al. 2013]. Die Arbeiten wurden am iVA in den Projekten QualiSaR und StandOrt sowie in Normungsgremien fortgesetzt.

2.5.2 Domänenspezifische Zertifizierung satellitenbasierter Ortung

Bei einer Zertifizierung der satellitenbasierten Ortung für eine bestimmte Verkehrsdomäne ist der jeweils gültige normative Rahmen zu berücksichtigen. Bei Nutzung universeller Ansätze wie dem V-Modell [IEC 61508] ist eine Übertragbarkeit der Zertifizierung auf andere Verkehrsdomänen möglich.

Als Grundlage für eine mögliche Zertifizierung wurden im Projekt GALCERT die entsprechenden Prozesse der einzelnen Domänen analysiert [Seybold 2007; Schnieder et al. 2009a] und in [GAUSS Basisprojekt 2010] ein domänenübergreifender und strukturierter Zertifizierungsprozess für das Raum- und Bodensegment erstellt. Ergebnis der Analyse war, dass sich die grundlegenden Prozesse für Schienen-, Straßen- und Luftverkehr ähneln und somit Synergien genutzt werden können. In allen drei Domänen teilen sich die Verantwortlichkeiten hauptsächlich auf Hersteller, Gutachter und Sicherheitsbehörde auf. Der Ansatz sieht eine Aufteilung für verschiedene Segmente vor, dass sie von verschiedenen Herstellern stammen und von verschiedenen Organisationen betrieben werden können. Jedoch existiert bisher kein normierter Prozess, um Empfänger von Galileo oder anderer Ortungssysteme für dynamische Anwendungen zu zertifizieren. Daher ist die Zertifizierung des Empfängers als industrielle Komponente notwendig, was im folgenden Abschnitt betrachtet wird.

2.5.3 Zertifizierung industrieller Komponenten für den Schienenverkehr

In diesem Abschnitt wird der Stand der Technik der Zertifizierung industrieller Komponenten als Grundlage für die Entwicklung und Zertifizierung der satellitenbasierten Ortungseinheit dargestellt. COTS sind entsprechend der Sicherheitsphilosophie des Schienenverkehrs unsicher und können somit zunächst nicht für sicherheitsrelevante Anwendungen genutzt werden.

Deren Nutzung für sichere Anwendungen im Schienenverkehr kann jedoch sinnvoll sein, wenn die Entwicklung einer Komponente mit ähnlichen Funktionen zu kostspielig oder im gewünschten zeitlichen Rahmen nicht möglich wäre. Die Nutzung industrieller Komponenten bietet zudem den Vorteil der modularen und flexiblen Ausstattung von Systemen [Bornschlegl 2014], so dass Komponenten bei Bedarf – bspw. wenn das Ende ihrer Lebenszeit erreicht ist oder sich die entsprechenden Anforderungen ändern – ausgetauscht werden können. Zudem lässt sich eine redundante Systemarchitektur bei einem modularen Aufbau eines Systems leichter erstellen als bei einem starren, unflexiblen Aufbau [Bornschlegl 2014].

Das Clearguard Axel Counter Module 200 (ACM 200) und das Track Circuit Modul 100 (TCM 100) wurden bspw. von Siemens unter Nutzung von COTS Hardwarekomponenten für Stromversorgung und Schnittstellen entwickelt. Deren Aufgabe ist die Überwachung eines Gleisabschnitts und die Übermittlung dessen Zustands an das Stellwerk [Körkemeier 2013; Körkemeier et al. 2013]. Auch die „Control Safe Platform“ der Firma Artesyn besteht aus COTS, so ist bspw. die CPU ein industrielles Bauteil. Die Aufgabe der Plattform ist die Reaktion im Störungsfall, so soll bspw. das Stellen des Blocksignals auf Halt gewährleistet werden. Die Zertifizierung erfolgte entsprechend SIL 4. Zur kosteneffizienten Herstellung und Entwicklung von Stellwerken hat das niederländische EIU ProRail von der Firma HIMA ein SPS Stellwerk entwickeln und herstellen lassen. Das HIMAX Steuersystem, ein wesentlicher Bestandteil des SPS-Stellwerks, ist mit SIL 4 zertifiziert [Blaauboer et al. 2013].

GSM-R und EBuLa werden bereits seit einem längeren Zeitraum im Schienenverkehr als COTS genutzt. Bei GSM-R wurden zur Gewährleistung der Sicherheit gemäß den Anforderungen des Schienenverkehrs entsprechende Protokolle eingeführt. Ein ähnliches Vorgehen wurde bei der Einführung des Elektronischen Buchfahrplans und Langsamfahrstellen (EBuLa) angewandt [Schaffarczik 2002]. Die Sicherheit des EBuLa kann nicht entsprechend den Anforderungen des Schienenverkehrs gewährleistet werden, daher wurden Rückfallebenen implementiert.

COTS werden derzeit bereits im Schienenverkehr genutzt, jedoch hauptsächlich für infrastrukturseitige Anwendungen. Dadurch werden sinkende Produktpreise aufgrund verteilter Entwicklungskosten auf viele Marktteilnehmer erhofft, was zur Erhöhung der Attraktivität des Schienenverkehrs beitragen soll. Zusätzlich kann bei der Verwendung von COTS die Entwicklung deutlich beschleunigt werden. Komponenten oder Sensoren müssen nicht neu entwickelt werden, es kann auf bestehende Lösungen zurückgegriffen werden. Bei einer notwendigen Modifizierung der Industriekomponenten spricht man von modifizierten Industriekomponenten (Modifiable off-the-shelf – MOTS). Dabei wird eine Industriekomponente in wesentlichen Teilen belassen, jedoch auf die individuellen Bedürfnisse der Anwendung angepasst. Moderne Entwicklungen im Elektronik- und Softwaresektor können somit schneller genutzt werden, dennoch werden COTS und MOTS im Schienenverkehr derzeit nur vereinzelt genutzt.

3 Normativer Rahmen

Für die sicherheitsgerichtete Entwicklung und Zertifizierung von Systemen ist im normativen Rahmen der einzuhaltende Ablauf und für die Entwicklung relevante Spezifikationen festgelegt. Zu dessen Kenntnis werden in Abschnitt 3.1 die Institutionen eingeführt, die an der Erstellung derartiger Dokumente beteiligt sind. Darauf aufbauend wird der Wandel der Normung und Legislative in Europa und dessen Einfluss auf die Entwicklung und Zertifizierung erläutert. In Abschnitt 3.2 werden die durch diese Institutionen erstellten Dokumente eingeführt. Darauf aufbauend wird in Abschnitt 3.3 die notwendige durchzuführende Sicherheitsnachweisführung detailliert betrachtet. In Abschnitt 3.4 werden die Anforderungen extrahiert, welche an Entwicklungen im Schienenverkehr gestellt werden. Mit diesem Vorgehen wird gewährleistet, dass alle für Entwicklung und Zertifizierung notwendigen Dokumente identifiziert und deren Anforderungen an einen sicheren Schienenverkehr mit satellitenbasierter Ortung berücksichtigt werden. Damit soll mit vertretbaren Maßnahmen und den zur Verfügung stehenden Ressourcen der Eintritt von Gefährdungen verhindert werden.

3.1 Entwicklung normativer Dokumente

Normen entstehen im Konsens durch Normungsgremien, die Mitglied internationaler oder nationaler Normungsorganisationen sind und an denen alle interessierten Kreise teilnehmen können. Weitere Grundsätze der Normungsarbeit sind Freiwilligkeit, Öffentlichkeit, Sachbezogenheit, Einheitlichkeit und Widerspruchsfreiheit, Ausrichtung am Stand der Technik, den wirtschaftlichen Gegebenheiten und am allgemeinen Nutzen sowie Internationalität [Reinbold 2007]. Durch die regelmäßige Überprüfung der Normen hinsichtlich ihrer Aktualität bilden diese den Stand der Technik ab. So wurde bspw. durch [DIN EN 50128] aus 2012 eine ältere Version aus 2001 ersetzt.

Um die bestehenden normativen Dokumente einordnen zu können, werden zunächst die dafür notwendigen Organisationen und deren historische Entwicklung betrachtet. Dafür werden die am Normerstellungs- (Abschnitt 3.1.1) und Gesetzgebungsprozess (Abschnitt 3.1.2) beteiligten Organisationen sowie Verbände, die ihre Interessen und die deren Mitglieder in die entsprechenden Prozesse einbringen (Abschnitt 3.1.3), eingeführt. Darauf aufbauend wird die historische Entwicklung der entsprechenden Dokumente mit Fokus auf den Wandel durch die in Europa gewünschte und geforderte Interoperabilität dargestellt (Abschnitt 3.1.4). Anschließend wird der Wandel der notwendigen Entwicklungsprozesse (Abschnitt 3.1.5) und der Einfluss des rechtlichen Wandels auf die Entwicklung und Zertifizierung (Abschnitt 3.1.6) betrachtet.

3.1.1 Beteiligte Organisationen am Normerstellungsprozess

Verschiedene Normungsorganisationen gewährleisten die Aktualität der normativen Dokumente und damit das Widerspiegeln des Stands der Technik. In Europa werden Normen von unabhängigen Organisationen wie dem Europäischen Komitee für Normung (Comité Européen de Normalisation – CEN), dem Europäischen Institut für Telekommunikationsnormen (European Telecommunications Standards Institute – ETSI) oder dem Europäischen Komitee für elektrotechnische Normung (Comité Européen de Normalisation Électrotechnique – CENELEC) erstellt. In den USA erteilt die staatliche Verkehrsbehörde den Auftrag zur Normerstellung, was vom Railroad Safety Advisory Committee durchgeführt wird. In Russland ist das Normungsorgan dem Ministerium für Wirtschaft und Handel unterstellt, dort werden die entsprechenden Arbeiten in Normungsgremien organisiert.

Das CEN erstellt Normen für alle Wirtschaftsbereiche, die in 33 Mitgliedsstaaten gültig sind [CEN 2010]. Durch die Mitgliedschaft in der Internationalen Organisation für Normung (ISO) werden internationale Interessen vertreten und Normen übernommen, das Deutsche Institut für Normung (DIN) vertritt dabei die deutschen Interessen.

Für Normen der Informations- und Kommunikationstechnologie ist das ETSI zuständig [ETSI 2012a], ihre Dachorganisation ist die internationale Fernmeldeunion (International Telecommunication Union – ITU).

Der Zuständigkeitsbereich des CENELEC ist die Normung im Bereich der Elektrotechnik, die internationale Dachorganisation ist die Internationale Elektrotechnische Kommission (Internationale Elektrotechnische Kommission – IEC) [CENELEC 2013], die deutschen Interessen werden durch die Deutsche Kommission Elektrotechnik Elektronik Informationstechnik (DKE) vertreten.

3.1.2 Beteiligte Organisationen im Gesetzgebungsprozess

Die Europäische Kommission (European Commission – EC) mit Hauptsitz in Brüssel ist die Exekutive der EU und vertritt deren Interessen. Sie schlägt dem Europäischen Parlament Gesetze vor, ist zuständig für die Durchsetzung verabschiedeter Gesetze und vertritt die EU außerhalb Europas [EC 2013b]. Nationale Gesetze werden von nationalen Parlamenten verabschiedet.

Die durch die Verordnung [EU/2004/881] geschaffene Europäische Eisenbahnagentur (European Railway Agency – ERA) hat durch den Entwurf von Richtlinien und Verordnungen eine bedeutende Stellung im Gesetzgebungsverfahren. So hat sie die TSI

[EU/2008/57], die Methoden des Sicherheitsmanagements (Common Safety Methods – CSM) und die Sicherheitsziele (Common Safety Targets – CST) erstellt und ist mit deren Überwachung beauftragt. Weiterhin sind der Austausch sicherheitsrelevanter Informationen sowie die Anwendung eines Risikomanagementverfahrens betroffen [Schweinsberg 2011]. Dabei soll die gegenseitige Anerkennung der Ergebnisse von Risikobewertungen erleichtert werden. Die CSM gelten dabei für den Neu- oder Umbau von Schienenfahrzeugen bzw. der Schieneninfrastruktur sowie die Änderung von Betriebsverfahren, wenn diese signifikant und sicherheitsrelevant sind. Sie richtet sich somit an Hersteller, Fahrzeughalter und Betreiber, die zur Nutzung verpflichtet sind [EU/2009/352].

3.1.3 Beteiligte Interessenverbände

Im Rahmen der Lobbyarbeit bringen verschiedene Organisationen ihre Interessen in den Normerstellungs- und Gesetzgebungsprozess ein, bspw. die Gemeinschaft der Europäischen Bahnen (Community of European Railway and Infrastructure Companies – CER), welche für 75 europäischen EVU und EIU im Europäischen Parlament, in der EC und im EU-Ministerrat vertreten ist. Durch ihre anerkannte Stellung wird die CER als Sprachrohr der Europäischen Eisenbahnen betrachtet.

Um ihre Interessen vertreten zu können, haben sich Hersteller zum Verband der europäischen Eisenbahnindustrie (Union des Industries Ferroviaires Européennes – UNIFE) zusammengeschlossen. Deren für Signaltechnik zuständige Arbeitsgruppe ist die UNISIG (Union Industry of Signalling). Die Vereinigung von EVU, EIU und Holdings im Schienenverkehr ist der Internationale Eisenbahnverband (Union internationale des chemins de fer – UIC).

3.1.4 Wandel der europäischen Legislative

Der normative und legislative Rahmen des Schienenverkehrs in Europa befindet sich seit etwa 1990 mit dem Ziel der Liberalisierung und Harmonisierung in einem steten Wandel. Dabei wurden bspw. nationale durch europäische Gesetze ersetzt. Dieser Prozess, der auch die Trennung von Infrastruktur und Betrieb und den diskriminierungsfreien Zugang von EVU zur Infrastruktur vorsieht, ist noch im Gange. Das EVU soll die Verantwortung für den sicheren Betrieb der Fahrzeuge übernehmen [Heinisch/Schweinsberg 2003], das EIU für die Sicherheit der Infrastruktur [EU/2011/217]. Damit wird zur Interoperabilität und somit zur Steigerung der Wettbewerbsfähigkeit beigetragen. Derzeit stellen nationale Regeln Markteintrittsbarrieren durch resultierende divergierende Technologien und Genehmigungsverfahren dar. Neben der betrieblichen Liberalisierung des

Schienenverkehrs in Europa wird die technologische Harmonisierung vorangetrieben. Mit den TSI soll auch das Kosten-Nutzen-Verhältnis von Entwicklungsprozessen im Schienenverkehr verbessert werden [EU/2011/217]. Die entsprechende Entwicklung der letzten Jahrzehnte ist in Abbildung 3-1 zusammengefasst. Die Prinzipien der europäischen Eisenbahnpolitik sind in den von der EU initiierten Eisenbahnpaketen verankert. Im ersten Eisenbahnpaket wurde der Zugang zur Nutzung der Eisenbahninfrastruktur geregelt.

Im zweiten Eisenbahnpaket wurde ein gemeinsames europäisches Sicherheitskonzept festgeschrieben, die Interoperabilität im Schienenverkehr geregelt [EU/2004/49] und die Gründung der ERA beschlossen. Weiterhin wurde festgelegt, das EVU und EIU mit einem Sicherheitsmanagementsystem (SMS) nachweisen müssen, dass sie den gesetzlichen Anforderungen entsprechen und qualifiziertes Personal einsetzen. Die resultierende Sicherheitsbescheinigung ist regelmäßig zu aktualisieren [EU/2004/49]. In [EU/2004/49] wird zudem die Entwicklung eines harmonisierten Ansatzes zur Risikobewertung gefordert, woraus die Verordnung über CSM entstanden ist [EU/2009/352]. Dort wird festgelegt, dass nach einer Identifikation der Gefährdungen die Risikoanalyse und -bewertung aufbauend auf bestehenden Risikoakzeptanzkriterien durchzuführen ist und daran der Nachweis der Übereinstimmung des Systems mit den identifizierten Sicherheitsanforderungen anschließt.

Das dritte Eisenbahnpaket beschäftigt sich mit der Zertifizierung von Triebfahrzeugführern, legt Grundlagen für die weitere Marktöffnung im Schienenpersonenverkehr, zum Schutz der Rechte von Fahrgästen sowie zur Qualitätssteigerung des Schienengüterverkehrs.

Das vierte Eisenbahnpaket befindet sich derzeit in Planung. Im technischen Teil soll eine Reform der Sicherheitsbescheinigungen und Zertifizierungen geregelt werden. Durch technische und strukturelle Reformen soll die Öffnung der inländischen Personenverkehrsmärkte für den Wettbewerb fortgesetzt werden [Innotrans 2013].

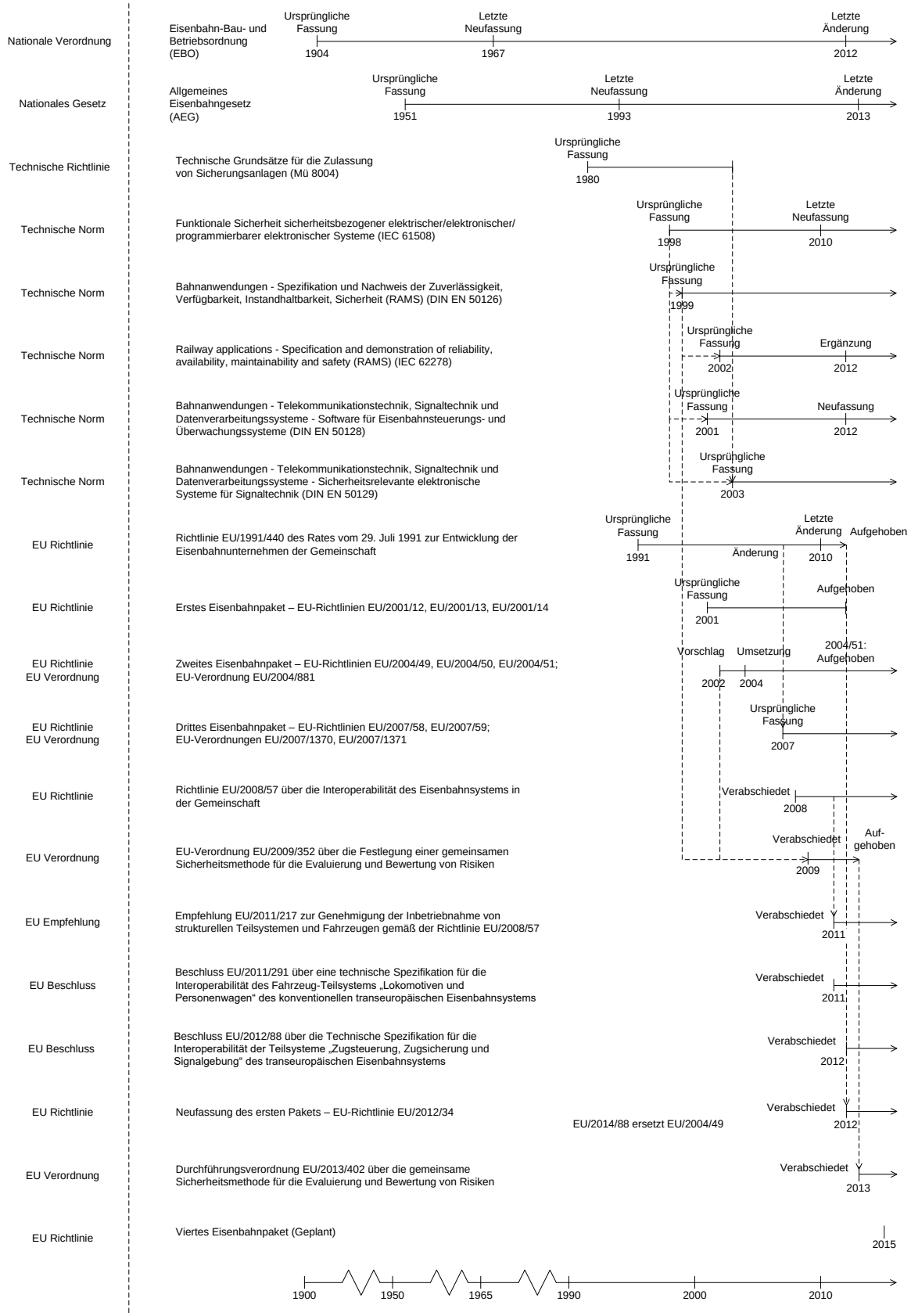


Abbildung 3-1: Legislative und normative Dokumente in der EU – historische Entwicklung

3.1.5 Wandel des sicherheitsgerichteten Entwicklungsprozesses

Aufgrund des gewünschten grenzüberschreitenden Verkehrs in der EU rückt die Zulassung von Schienenfahrzeugen mit verschiedenen Stromversorgungs- und Zugbeeinflussungssystemen für den Einsatz in mehreren Ländern verstärkt in den Fokus der Hersteller, Sicherheitsbehörden und Gutachter. Der dafür notwendige Entwicklungsprozess wird derzeit entsprechend den nationalen Anforderungen und Prozessen in den jeweiligen Nationalstaaten durchgeführt. Mittels gegenseitiger Anerkennung ist die Zertifizierung eines Mitgliedstaats in anderen Länder gültig (cross-acceptance). Damit kann eine wesentliche Verkürzung und Kostenersparnis der Entwicklung realisiert werden. Das entsprechende Produkt muss nicht in jedem Mitgliedsstaat separat zertifiziert werden, es müssen lediglich nationale Besonderheiten sowie Sonderfälle der TSI betrachtet werden. Dies kann jedoch auch zu einem langwierigen Prozess führen, abhängig davon wie verschieden die nationalen Besonderheiten sind und ob sich diese widersprechen. Die gegenseitige Anerkennung der Zertifizierung ist somit lediglich eine sinnvolle Übergangslösung bis ein finaler, länderübergreifender Entwicklungsprozess existiert.

3.1.6 Einfluss des rechtlichen Wandels auf die Entwicklung und Zertifizierung

In den bereits vor Beginn der europäischen Harmonisierung gültigen deutschen Gesetzen – dem Allgemeinen Eisenbahngesetz (AEG) und der Eisenbahn-Bau- und Betriebsordnung (EBO) – wird allgemein gefordert, dass Bahnanlagen und Fahrzeuge den Anforderungen der Sicherheit und Ordnung genügen müssen. Die allgemein anerkannten Regeln der Technik sind einzuhalten, ein Abweichen ist bei Nachweis der mindestens gleichen Sicherheit möglich [EBO 2012]. Technische Grundsätze wurden in der Richtlinie Mü 8004 vorgegeben [Mü 8004]. Der Betrieb ist unter der Eisenbahnaufsicht des Bundes zu führen, die auch die Fahrzeuge vor Inbetriebnahme und in Zyklen von maximal acht Jahren überprüft [EBO 2012]. Andere technische Aspekte sind hingegen sehr detailliert geregelt, bspw. dass eine Pfeife, eine Sicherheitsfahrschaltung und ein Zugfunk vorhanden sein müssen – ebenso ein Aschekasten bei Verwendung fester Brennstoffe [EBO 2012]. Dieses absolute Sicherheitsverständnis wird nun, auch normativ, von einer Akzeptanz des zulässigen Risikos im Schienenverkehr ersetzt, was mit einer Entwicklung nach einem vorgegebenen Prozess realisiert und über Ausfallraten nachgewiesen wird. Somit führte die europäische Harmonisierung zu einem Wandel vom regelbasierten zum anforderungsbasierten Ansatz und zu einer höheren Eigenverantwortung, die letztlich in einem erweiterten Gestaltungsspielraum des Herstellers mündet.

Die 2009 eingeführte CSM-Verordnung [EU/2009/352] wird in Deutschland durch die Sicherheitsrichtlinie Fahrzeug (SIRF) erfüllt. Mit dieser wird eine vollständige Regelung zum Nachweis der funktionalen Sicherheit in Schienenfahrzeugen getroffen [Rüsch 2012]. Zur Durchführung der Fahrzeugzulassungen in Deutschland entsprechend den europäischen Regelungen wird der in Deutschland gültige Prozess angepasst. Dafür wurde zwischen dem Bundesministerium für Verkehr und digitale Infrastruktur (BMVI), dem Eisenbahn-Bundesamt (EBA), der DB und der Bahnindustrie ein Memorandum of Understanding getroffen [BMVBS 2013]. Auf die daraus resultierenden Veränderungen der Verantwortlichkeiten wird in Abschnitt 4.1.4 eingegangen. Fahrzeuge, die ausschließlich auf TEN-Strecken verkehren, werden nach Anforderungen an Nachweis, Dokumentation und Prüfung des § 32 EBO zugelassen.

3.2 Zugrunde liegende Dokumente des normativen Rahmens

In den folgenden Abschnitten wird der für diese Arbeit bedeutende normative Rahmen dargestellt. Die in Abschnitt 3.2.1 eingeführten Industrienormen sind die Grundlage für eine sichere Systementwicklung. Zur Strukturierung der Anforderungen und des zu entwickelnden Systems werden in Abschnitt 3.2.2 Normen zur Systemklassifikation eingeführt. Aufgrund der geplanten Anwendung der Ergebnisse dieser Arbeit im Schienenverkehr werden in Abschnitt 3.2.3 die grundlegenden Normen der sicheren Entwicklung dieser Verkehrsdomäne eingeführt. Folgend auf den technischen Normen werden in Abschnitt 3.2.4 die grundlegenden Spezifikationen des Schienenverkehrs eingeführt. In Abschnitt 3.2.5 werden die beiden verbleibenden Kategorien, Dokumente des Herstellers und Betreibers, betrachtet. Abschließend erfolgt in Abschnitt 3.2.6 ein Blick auf die international für die Entwicklung im Schienenverkehr genutzten Dokumente.

Zur weiteren Verwendung in dieser Arbeit wird eine Strukturierung des normativen Rahmens eingeführt. Nach [Rüthers/Fischer 2010] und [Schnieder/Schnieder 2013] ist eine Unterteilung in verbindliche Rechtsvorschriften und unverbindliche technische Regeln sinnvoll. Die technischen Regeln haben dabei eine geringere Gültigkeit und Verbindlichkeit, jedoch einen höheren Grad der behördlichen Detaillierung. Aufgrund ihrer Anerkennung im entsprechenden Fachbereich sind sie jedoch von hoher Bedeutung. Eine Zusammenfassung des im Schienenverkehr gültigen normativen Rahmens entsprechend des in Abbildung 3-2 eingeführten Schemas ist in Abbildung 3-3 dargestellt, für die satellitenbasierte Ortung in Anhang 3.

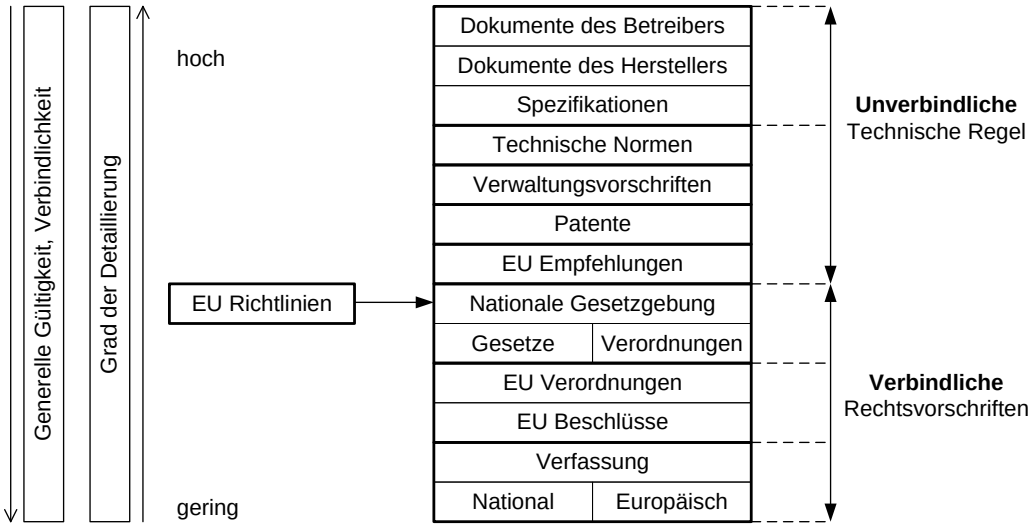


Abbildung 3-2: Struktur des normativen Rahmens nach [Rüthers/Fischer 2010; Schnieder/Schnieder 2013]

Derzeit ist die europäische Rechtsordnung parallel zu nationalen Verfassungen die Grundlage des normativen Rahmens. Europäische Rechtsvorschriften gelten immer einschließlich ihrer Fortschreibung, sie haben eine höhere Verbindlichkeit als nationale Gesetze. Eine vergleichbare Beziehung besitzt bspw. das Bundesrecht, welches über dem Landesrecht steht. Europäische Verordnungen sind bereits direkt unionsweit gültig, genau wie Beschlüsse, deren Gültigkeit sich jedoch auf bestimmte Fachbereiche beschränkt [AEUV 2010]. Richtlinien müssen in nationales Recht überführt werden, Empfehlungen haben keinen verbindlichen Charakter.

Unverbindliche technische Regeln haben als allgemein anerkannte Regeln der Technik eines Fachbereichs im Entwicklungs- und Zertifizierungsprozess eine besondere Bedeutung. Sie sind praktisch erprobt, durch die Mehrheit der Fachleute akzeptiert, wissenschaftlich begründet und passen sich der Entwicklung in einem Fachgebiet an [VV BAU-STE 4.6 2014]. Durch den Bezug zu Verordnungen haben Normen im europäischen Eisenbahnwesen eine hohe Verbindlichkeit.

3.2.1 Allgemeine Industrienormen

Neben dem speziellen normativen Rahmen des Schienenverkehrs und der satellitenbasierten Ortung sind für einen strukturierten, konsistenten und sicherheitsgerichteten Entwicklungsprozess allgemein gültige Normen von Bedeutung. Diese sind bspw. [DIN EN ISO 9000; DIN EN ISO 9001], welche für alle Industriebereiche Vorgaben für ein aufzubauendes und zu betreibendes Qualitätsmanagementsystem (QMS) festlegen, um die unternehmensinternen Prozesse und somit auch die Produktentwicklung nach allgemeinen Vorgaben durchzuführen.

3.2.2 Normen der Systemklassifikation

Als Kernnormen der Systemklassifikation wurden [DIN EN 81346-1; DIN EN 81346-2; DIN ISO 81346-3] identifiziert, welche gemeinsam von IEC und ISO veröffentlicht wurden und somit als allgemein gültig angesehen werden kann. Diese Normung „führt allgemeine Prinzipien zur Strukturierung von Systemen, einschließlich der Strukturierung von Informationen über Systeme ein“ [DIN EN 81346-1]. Zudem bildet sie die Grundlage für die Klassifizierung von technischen Objekten für alle Fachbereiche. Die Strukturierung eines technischen Systems muss dabei „auf Grundlage einer Bestandteil-von-Beziehung“ [DIN EN 81346-1] erfolgen. Dies impliziert die Forderung nach einer detaillierten Strukturierung. Diese wird präzise Definitionen enthalten, da diese notwendig sind, um sprachliche Problemfälle wie Inkonsistenz und Ambiguität, die den Prozess der Entwicklung und der späteren Zertifizierung erschweren können, zu vermeiden [Schnieder 2010].

Aufgrund der vorgesehenen Anwendung des eingeführten Vorgehens im Schienenverkehr werden zur detaillierten Strukturierung Normen dieser Verkehrsdomäne verwendet. Eine Systematik zur Kennzeichnung und Strukturierung von technischen Systemen im Schienenverkehr ist in [DIN EN 15380-1; DIN EN 15380-2; DIN EN 15380-3; DIN EN 15380-4; DIN EN 15380-5] zu finden. Eine Verwendung dieser Normengruppe erscheint sinnvoll, da bspw. bei der Definition von „Objekt“, „System“ und „produktbezogener Struktur“ in der Normengruppe DIN EN 15380 auf [DIN EN 81346-1] verwiesen wird, um eine Untergliederung zu erstellen. Diese Normen werden zur Systemstrukturierung in Abschnitt 4.3 genutzt.

3.2.3 Grundlegende Normen des Schienenverkehrs

Die grundlegenden Normen des Schienenverkehrs geben Anforderungen und Verantwortlichkeiten für den Entwicklungsprozess und die Zertifizierung vor, wofür sie in diesem Abschnitt identifiziert und betrachtet werden. Die Sicherheit, Zuverlässigkeit, Verfügbarkeit und Instandhaltbarkeit der Zugbeeinflussungstechnik werden in den Normen [DIN EN 50126], [DIN EN 50128] sowie [DIN EN 50129], die auf der [IEC 61508] aufbauen, betrachtet. Dort wird bspw. festgelegt, dass eine Systemdefinition als Grundlage für Entwicklung, Risikoanalyse und Betrieb stattfinden muss [DIN EN 50126]. In [DIN EN 50129] werden quantitative Gefährdungsraten eingeführt, gefordert und Verantwortlichkeiten definiert. Im Schienenverkehr existieren allgemeine Anforderungen, die von Schienenfahrzeugen und deren Komponenten erfüllt werden müssen. Die Anforderungen resultieren aus dem in Abbildung 3-3 dargestellten normativen Rahmen.

Abbildung 3-3: Normativer Rahmen im Schienenverkehr

3.2.4 Grundlegende Spezifikationen des Schienenverkehrs

Ebenfalls von Bedeutung für die Zertifizierung sind Spezifikationen, die bspw. von Behörden wie der ERA oder einem Konsortium aus mehreren Herstellern herausgegeben werden. Sie beschreiben technische Details eines Systems, wie das Subset 026 der UNISIG „ETCS Specifications“.

Ein Beispiel für Spezifikationen im Schienenverkehr sind die TSI, auf die im Folgenden aufgrund ihrer Bedeutung detailliert eingegangen wird. 1999 wurden die TSI separat für den konventionellen Schienenverkehr und für den Hochgeschwindigkeitsverkehr erstellt, bei ihrer jüngsten Überarbeitung wurde diese Trennung aufgehoben [Amt für Veröffentlichungen 2014]. Dabei ging die Kategorie „Zugsteuerung, Zugsicherung und Signalgebung“ (Control command and signalling – CCS) in der Kategorie „Schienenfahrzeuge“ (Locomotives and passenger – LOC&PAS) auf. Die derzeit gültigen TSI sind in Abbildung 3-4 zusammengefasst.

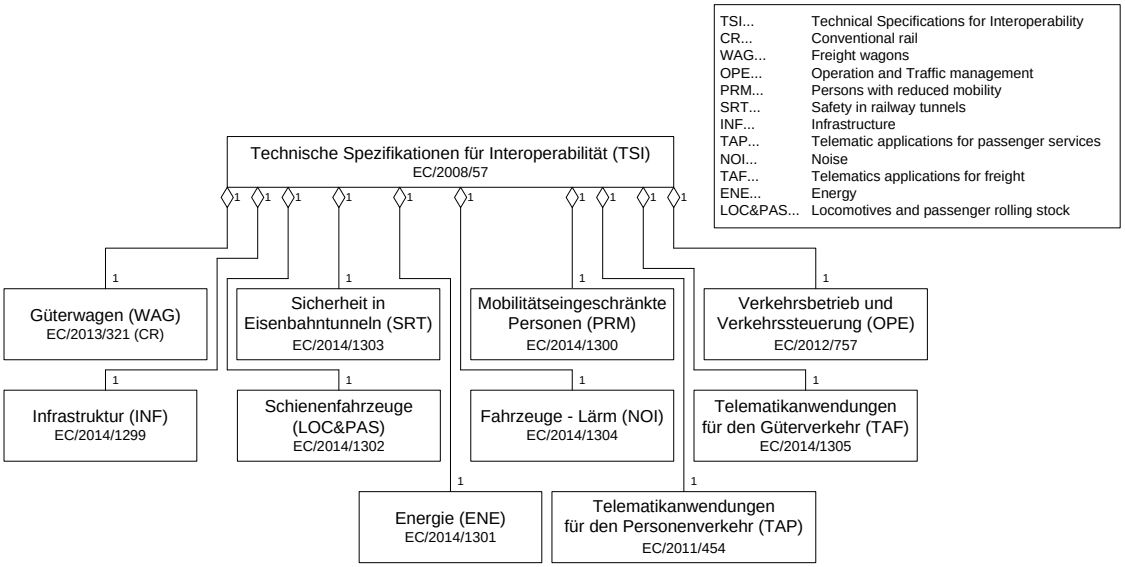


Abbildung 3-4: Übersicht der Technischen Spezifikationen für Interoperabilität mit Stand 1.1.2015 [ERA 2014; Amt für Veröffentlichungen 2014]

Die ersten TSI waren Richtlinien und mussten erst in nationales Recht umgesetzt werden, was in Deutschland durch die Transeuropäische Eisenbahn Interoperabilitäts-verordnung (TEIV) [TEIV 2004] geschah. Die neuesten TSI sind Verordnungen und damit unmittelbar in den Mitgliedsstaaten der EU gültig. Die Aktualität der TSI wird durch einen permanenten Verbesserungsprozess ermöglicht, in den Nutzer Vorschläge und Ergänzungen einbringen können [EU/2011/217].

Mit Hilfe der TSI soll primär die Migration zu ERTMS entlang der TEN-Korridore vorangetrieben werden. In Deutschland betrifft das für die primäre Integration von ERTMS die Korridore A (Rotterdam – Genua), B (Stockholm – Neapel), E (Dresden –

Konstanza) und F (Aachen – Terespol), wo zwischen den Grenzübergangspunkten zum benachbarten Ausland ERTMS streckenseitig einzurichten ist [TEIV 2004]. Ausnahmen können für Fahrten von nicht-TEN-Strecken in TEN-Bahnhöfe und für Projekte, die zum Zeitpunkt des Erlasses der TSI bereits weit vorangeschritten waren und somit die Wirtschaftlichkeit des Projektes gefährdet wäre, gelten.

Nationale Besonderheiten, bspw. bezüglich Fahrfähigkeit oder elektromagnetischer Verträglichkeit [EBA 2014] auf den TEN, werden durch die notifizierten nationalen technischen Regeln (Notified National Technical Rules – NNTR) geregelt, die entsprechend ihrer Gültigkeit über die Grenzen von Mitgliedsstaaten hinaus und ihrer Migrierbarkeit in die TSI kategorisiert werden [EU/2008/57]. Die NNTR, welche der ERA zur Kenntnis zu übermitteln sind, hemmen derzeit die grenzüberschreitende Zulassung von Schienenfahrzeugen. Daher ist das Ziel der EU, diese abzubauen [EU/2011/217], um eine direkte Zulassung in der EU ohne nationale Prüfung zu ermöglichen. Um sich diesem Ziel zu nähern, wurde die Anzahl der NNTR von 300 (2012) auf 80 (2014) reduziert [Steindl 2015].

3.2.5 Dokumente des Herstellers und Betreibers

Der Hersteller und der zukünftige Betreiber erstellen diverse Dokumente, die während der Entwicklung von Bedeutung sind. Das sind allgemeingültige Dokumente wie ein Qualitäts- und Sicherheitsmanagementplan sowie ein Verifizierungs- und Validierungsplan.

Dokumente des Betreibers beziehen sich auf die Durchführung des täglichen Verkehrs. Ein Beispiel dafür ist die Ril 915 „Bremse im Betrieb bedienen und prüfen“ der DB, die in [VDV Schrift 757] aufgegangen ist, um für alle EVU ein gemeinsam abgestimmtes, einheitliches Regelwerk zu schaffen. Dokumente des Herstellers, bspw. Spezifikationen, dienen der Beschreibung und Zertifizierung von Komponenten, welche im Schienenverkehr eingesetzt werden, was der Sicherheitsnachweis sein kann.

Im Lastenheft stellt der Betreiber seine Anforderungen an das Produkt dar. Freigegebene Lastenhefte werden nach [VV NTZ ÜGR Stufe 2 2013] als anerkannte Regeln der Technik behandelt. Darauf aufbauend erstellt der Hersteller das Pflichtenheft, in dem die Umsetzung der gestellten Anforderungen im Projektverlauf beschrieben wird [VV NTZ ÜGR Stufe 2 2013]. Auch Dokumente, die Zulieferteile beschreiben, sind bedeutende der Entwicklung zugrunde liegende Dokumente. Derartige Referenzdokumente sind bspw. die Spezifikation von Sensoren.

3.2.6 Internationale Dokumente der Entwicklung im Schienenverkehr

Um von den Erfahrungen auf anderen Kontinenten zu profitieren, werden in diesem Abschnitt beispielhaft die für einen Entwicklungsprozess und die darauf folgende Zertifizierung im Schienenverkehr in den USA notwendigen Dokumente betrachtet.

Für Zertifizierung in den USA ist die Federal Railroad Administration (FRA) zuständig, die auf europäische, internationale und militärische Normen sowie Standards zurückgreift. Von den aus den USA stammenden, aber international gültigen Standards, beschreibt die IEEE 1474.1:2004 die Anforderungen an kommunikationsbasierte Zugbeeinflussungssysteme, welche Ortung und kontinuierliche, bidirektionale Datenübertragung beinhaltet [Standard 1474.1]. Der Standard IEEE 1483:2000 wird unter anderem bei sicherheitskritischen Anwendungen im Schienenverkehr genutzt [Standard 1483]. [MIL STD-882E] wird für Risikoanalysen von Soft- und Hardware verwendet und kann damit auch im Schienenverkehr eingesetzt werden. Anhand dieser Analyse wird deutlich, dass in den USA auf Normen bzw. Standards anderer Bereiche zurückgegriffen wird, im Gegensatz zu Europa wo im Eisenbahnwesen die Nutzung von Normen außerhalb des Schienenverkehrs unüblich ist. Die Nutzung von Normen außerhalb des Schienenverkehrs erlaubt eine vielfältigere Zertifizierung. Der europäische Ansatz soll eine höhere Qualität gewährleisten.

3.3 Sicherheitsnachweisführung

Die Sicherheitsnachweisführung wird nach den anerkannten Verfahren und Regeln durch den Hersteller durchgeführt. Im von ihm erstellten SICHERHEITSNACHWEIS, der von einem Gutachter geprüft wird, dokumentiert er nachvollziehbar seine getroffenen Annahmen bezüglich des Systems, Teilsystemen oder einzelner Komponenten auf Grundlage des zu Beginn der Entwicklung festgelegten Stands der Technik.

> „Der Sicherheitsnachweis ist ein dokumentierter Nachweis darüber, dass ein Produkt die gesetzlichen und spezifizierten Sicherheitsanforderungen erfüllt.“ [Schnieder/Schnieder 2013]

Es wird nachgewiesen, mit welchen Maßnahmen das Sicherheitsniveau der Systemfunktionen erreicht wurde [Schnieder/Schnieder 2013] und wie das System trotz Gefährdungen von innen und außen einen sicheren Betrieb gewährleistet. Um industrielle Komponenten, also bspw. die satellitenbasierte Sensorik, integrieren zu können, werden hier die bestehenden Ansätze aus verschiedenen Domänen als methodische Grundlage betrachtet. Zunächst werden in Abschnitt 3.3.1 für diese Arbeit wesentliche Begriffsdefinitionen eingeführt. Der Sicherheitsnachweis aus der Verkehrsdomäne Luftfahrt wird in Abschnitt 3.3.2 und der Sicherheitsnachweis im Schienenverkehr wird

in Abschnitt 3.3.3 betrachtet, außerhalb des Verkehrs werden die Wehrtechnik und die Gesundheitsbranche identifiziert. Um entsprechend den Ziele dieser Arbeit den Schienenverkehr zu fokussieren, wird in Abschnitt 3.3.4 der Einfluss der TSI dargestellt und in Abschnitt 3.3.5 der Stand der Technik der Sicherheitsnachweisführung im Schienenverkehr weltweit betrachtet. In Abschnitt 3.3.6 wird ein domänenübergreifender Ansatz eingeführt. In Abschnitt 3.3.7 wird eine Methode zur Strukturierung der Sicherheitsnachweisführung dargestellt, in Abschnitt 3.3.8 werden die Ansätze schließlich zusammengefasst.

In der Wehrtechnik ist Sicherheit von hoher Bedeutung, da der Einsatz bspw. von Schusswaffen mit höchster Präzision zu erfolgen hat, um keine unbeabsichtigten Gefährdungen hervorzurufen. Der betrachtete Sicherheitsnachweis im Gesundheitswesen betrifft den Umgang mit Sonderabfällen – es sollen keine Gefährdungen für Leib und Leben bei damit durchgeführten Arbeiten entstehen. Der Sicherheitsnachweis besteht in allen Domänen aus Sicherheitsbehauptungen, Nachweisen, Verifizierung, Validierung und einer schlüssigen Argumentationskette, wofür Annahmen getroffen werden und das System abgegrenzt werden muss [Defence Standard 00-56]. Für die betrachtete Anwendung mit definierten Anwendungsbedingungen wird eine stringente und verständliche Beweisführung durchgeführt [Defence Standard 00-56].

Eine Gemeinsamkeit der Sicherheitsnachweise liegt zudem in ihrer Entstehung – ihre Verbesserung basiert auf Erkenntnissen, die durch Unfälle gewonnen wurden. Die Systementwicklung erfolgt mit größter Sorgfalt, jedoch basiert die Entwicklung meist auf dem Wissen bekannter Fehler, weshalb nur diese vermieden werden können. Der Ansatz von [Leveson 2012] versucht eine Systementwicklung zu etablieren, ohne dafür vorher eingesetzte Fehler nutzen zu müssen, indem durch eine Modellierung von vornherein Fehler ausgeschlossen werden [Ericson 2005]. Ein entsprechender Ansatz für die Automobilindustrie wurde in [Ständer 2010] erarbeitet.

3.3.1 Begriffsdefinitionen

Aus vorangegangenen wissenschaftlichen Arbeiten ist bekannt, dass sich die Terminologien der satellitenbasierten Ortung und die des Schienenverkehrs unterscheiden [Schnieder 2010; Stein 2012; Wegener 2013; Lu 2014; Yurdakul 2016]. So existiert bspw. der Begriff Sicherheit nicht in der Domäne satellitenbasierte Ortung [EC/ESA 2002]. Aufgrund der Nutzung der in dieser Arbeit betrachteten satellitenbasierten Ortungseinheit in einem SCHIENENFAHRZEUG auf einer INFRASTRUKTUR wird die Terminologie des Schienenverkehrs fokussiert.

> Ein Schienenfahrzeug ist ein „spurgebundenes Fahrzeug, das auf Gleisen geführt und getragen wird.“ [DIN EN 15380-1]

> Infrastruktur ist ein „System von Einrichtungen, Ausrüstungen und Dienstleistungen, das für den Betrieb einer Organisation erforderlich ist.“ [DIN EN ISO 9000]

Dafür werden in dieser Arbeit die notwendigen PROZESSE basierend auf den normativen ANFORDERUNGEN beschrieben.

> Ein Prozess ist die „Gesamtheit von aufeinander einwirkenden Vorgängen in einem System, durch die Material, Energie oder Information umgeformt, transportiert oder gespeichert wird.“ [DIN EN 81346-1]

> Anforderungen sind „notwendige Bedingung oder Vermögen, um die Lösung einer Aufgabe oder eines Zieles einzuschränken.“ [DIN EN 15380-5; DIN EN 15380-4]

Die Zulassung ist nach der Integration einer oder mehrerer zertifizierter Komponenten in das Gesamtumfeld eines Systems die Bestätigung, dass das System sicher genutzt werden kann. Hierbei kann die Entscheidung über die Nutzung von einer Behörde, einer Institution oder einem Gremium kommen [DIN EN 50126].

Die Zertifizierung ist ein Nachweis, der die Einhaltung von Spezifikationen, Normen, Anforderungen und Vertragsbedingungen bestätigt und den Abschluss des Entwicklungsprozesses darstellt, sie kann auch als Teilsystemzulassung bezeichnet werden [DIN EN ISO/ IEC 17065]. Die Entwicklung mündet in der Zertifizierung eines Systems, daher besteht zwischen diesen beiden Prozessen eine enge Verknüpfung. Die Institution, welche die Zertifizierung vornimmt, muss dafür unabhängig akkreditiert sein, wofür die nationale Akkreditierungsstelle, in Deutschland die DAkkS (Deutsche Akkreditierungsstelle), zuständig ist [DIN EN ISO/ IEC 17011]. Die Akkreditierung ist somit die offizielle Anerkennung der Möglichkeit eines Unternehmens, einer anderen Institution die Erfüllung von Prozessen oder Fähigkeiten nachzuweisen [Hänsel 2008].

Aufgrund dieser Definitionen wird im weiteren Verlauf dieser Arbeit der Entwicklungsprozess betrachtet, der in die Zertifizierung übergeht und mit dieser in Interaktion steht. Ziel dessen ist die Typzulassung und somit die Integration der Ortungseinheit in ein zuzulassendes oder zugelassenes Fahrzeug, was jedoch nicht Bestandteil dieser Arbeit ist.

3.3.2 Sicherheitsnachweis in der Luftfahrt

In der Luftfahrt wird mit einer Vielzahl von technischen und organisatorischen Maßnahmen das Ziel verfolgt, die Unfallrate stetig zu senken. So soll das Sicherheitsmanagement von der mittleren und oberen Führungsebene durchgeführt werden, da dort ein besonderes Maß an Erfahrung erwartet wird [Edwards 2000]. Der sichere Betrieb wird dabei durch die Einführung eines SMS gewährleistet, was den Umgang mit Risiken zu einem integralen Bestandteil der Prozesse eines Unternehmens macht. Die Sicherheitsbetrachtung sollte zu Beginn der konzeptionellen Entwicklungsphase durchgeführt werden [SAE 1996; SAE 2010]. Der strukturierte Ansatz zur Bewertung und Kontrolle von Gefährdungen wird dabei als Gefährdungsmanagement bezeichnet.

Ein Sicherheitsnachweis als Teil des Sicherheitsmanagements ist ein systematischer und strukturierter Nachweis der sicheren Durchführung des Luftverkehrs mit verständlichen Beweisen und Argumenten [Edwards 2000]. Dafür werden Gefährdungen identifiziert und bewertet und Wege aufgezeigt, wie mit diesen vernünftig umgegangen werden kann [DO 254]. Dieses Vorgehen ist wesentlich, da es bei geringer Eintrittswahrscheinlichkeit möglicherweise nicht lohnenswert ist, bedeutende Ressourcen in die Beseitigung der Gefährdung zu investieren, bei potentiell häufig auftretenden Gefährdungen verhält es sich entsprechend umgekehrt. Damit soll sichergestellt werden, dass lediglich ein akzeptables Risiko eingegangen wird, was als Zielvorgabe der Sicherheit oder momentan akzeptiertes Niveau betrieblicher Sicherheit bezeichnet wird [Fowler 2005].

Die strukturierte Dokumentation des Sicherheitsnachweises dient dabei nicht nur dem Nachweis der Sicherheit als Teil des Entwicklungsprozesses, die Nachverfolgbarkeit zwischen den Dokumenten ist dabei von besonderer Bedeutung [DO 178C]. Darüber hinaus wird die Darstellung des Nutzens des betrachteten Produkts gegenüber Interessenvertretern inner- und außerhalb eines Unternehmens sowie der Nachweis der Produktentwicklung entsprechend dem Stand der Technik insbesondere nach Unfällen ermöglicht [Fowler 2005]. Damit soll ermöglicht werden, dass die zivile Luftfahrt ihre hohen Sicherheitsansprüche weiterhin erfüllen kann.

3.3.3 Sicherheitsnachweis im Schienenverkehr in Europa

Der Sicherheitsnachweis oder safety case im Schienenverkehr wird vom Hersteller erstellt und dient dem Gutachter zum Verständnis des entwickelten Systems [May 2010; Schnieder et al. 2011; EBA 2012; Pachl 2013]. Ein Dokumentenmanagementsystem mit Review, Freigabe, Versionierung, Referenzierung und Nachverfolgbarkeit ist dabei selbstverständlich, um die Konsistenz der Dokumentation zu erhöhen und die Anzahl der

Fehler zu reduzieren. Der sicherheitsgerichtete Entwicklungsprozess soll das Auftreten menschlicher Fehler durch technische Maßnahmen in jeder Phase des Lebenszyklus reduzieren [Bikker/Schroeder 2002; Braband 2006]. Das System soll angemessen sicher für die vorgesehene Verwendung sein. Das geschieht durch die Reduzierung systematischer Fehler im System, Subsystem und deren Komponenten [Braband 2005].

Verweise auf bereits zertifizierte Systeme und die dort angewandten Sicherheitsprinzipien sind hilfreich und erleichtern die Begutachtung und Zertifizierung [Schnieder et al. 2011]. Dies schließt den Nachweis der Sicherheit der entwickelten und verwendeten Hard- und Software ein, die entwicklungsbegleitend zu dokumentieren ist [DIN EN 50129]. Der Sicherheitsnachweis besteht aus sechs Teilen, die zusammenfassend in Abbildung 3-5 dargestellt und im Folgenden detailliert beschrieben werden.

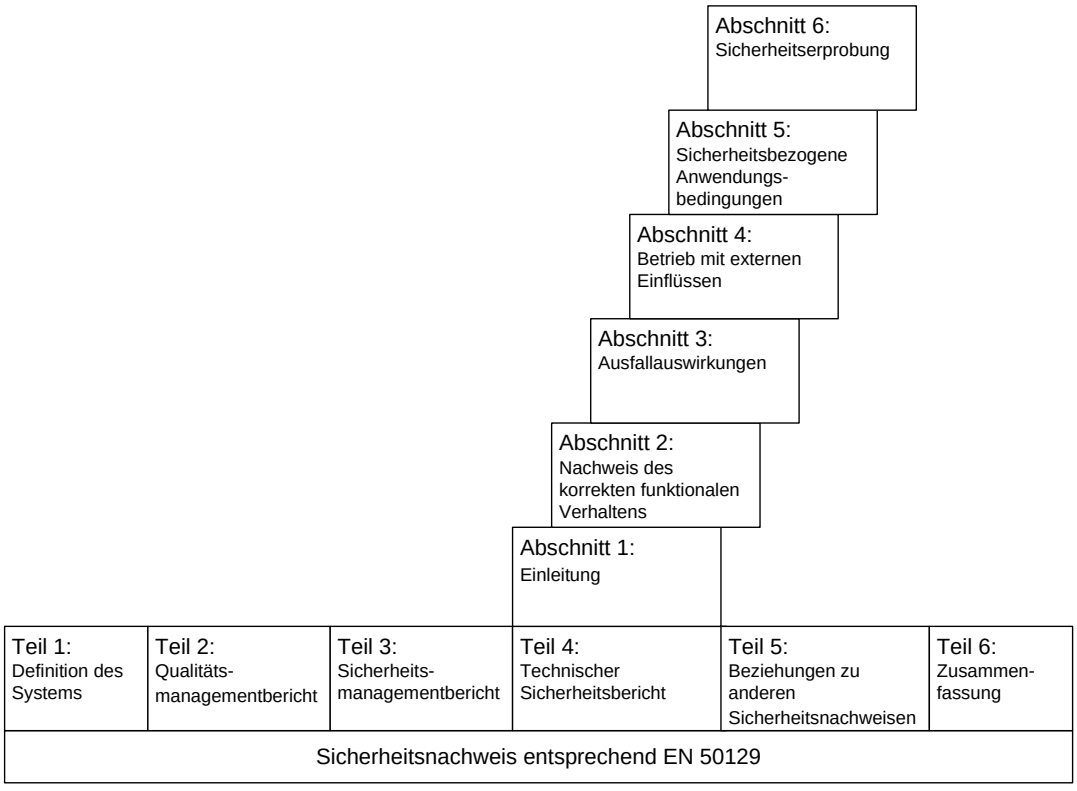


Abbildung 3-5: Struktur des Sicherheitsnachweises entsprechend des normativen Rahmens [DIN EN 50129; May 2010]

Im ersten Teil (Definition des Systems) wird das System, für welches der Sicherheitsnachweis durchgeführt werden soll, und seine grundlegenden Funktionen beschrieben, dargestellt, erläutert und genau definiert. Die genutzte Soft- und Hardware muss zusammen mit den notwendigen Dokumenten und Systemanforderungen methodisch detailliert beschrieben werden, wozu sich entsprechende Tools empfehlen, welche das System beschreiben [Bikker/Schroeder 2002].

Der zweite (Qualitätsmanagementbericht) und dritte (Sicherheitsmanagementbericht) Teil des Sicherheitsnachweises sind Standarddokumente des Herstellers [DIN EN 50129]. In diesem muss die im Unternahmen verankerte Qualitäts- und Sicherheitskultur nachgewiesen werden.

Die Hersteller weisen ihr QMS anhand eines Zertifikats nach [DIN EN ISO 9001]. Zusätzliche Anforderungen an die QMS von Bahnherstellern und Zulieferer von Komponenten werden durch die IRIS (International Railway Industry Standard) Zertifizierung gestellt, welche mit Stand 1.5.2015 1150 Unternehmen erteilt war [UNIFE 2016]. Mit dem Nachweis des Qualitätsmanagements wird sichergestellt, dass die „Qualität des Systems, Teilsystems oder der Einrichtung ... über den gesamten Lebenszyklus gewährleistet wird“ [DIN EN 50129]. Dieses Vorgehen erfolgt, um das Risiko menschlichen Versagens und von systematischen Fehlern in Systemen, Teilsystemen oder der Einrichtung in allen Phasen des Lebenszyklus zu reduzieren. Um den gesamten Lebenszyklus zu berücksichtigen, werden bspw. Organisationsstruktur, Qualitätsplanung und -verfahren, Inspektion und Tests, Mitarbeiterkompetenz und Ausbildung sowie Stilllegung und Entsorgung berücksichtigt. Die Betrachtung der Sicherheit in den einzelnen Phasen des Lebenszyklus ermöglicht es, risikoreduzierende Faktoren exakt an den geeigneten Stellen zuzuordnen [Slovak 2006]. Zudem ist nachzuweisen, dass eine adäquate Dokumentation der Entwicklungsphase und der Sicherheitsplanung gewährleistet ist [DIN EN 50129].

Im Sicherheitsmanagementbericht, welcher für SIL 1 bis 4 verbindlich ist, wird der Sicherheitsmanagementprozess des Herstellers, der für all seine Entwicklungen genutzt wird, dargestellt. Darin ist eine klare Aufteilung der Verantwortlichkeiten, eine konsistente Sicherheitsplanung, das konsistente Führen eines Gefährdungslogbuches, die Dokumentation der Sicherheitsanforderungsspezifikationen und der damit zusammenhängende Systementwurf, eine kontinuierliche Sicherheitsbegutachtung und eine unabhängige Sicherheitsverifizierung und -validierung nachzuweisen [Fenner et al. 2003; Schnieder/Schnieder 2013]. Auch sind Maßnahmen zur Übergabe an den Betreiber sowie zu Betrieb, Instandhaltung, Stilllegung und Entsorgung vorzusehen. Das dokumentierte Sicherheitsmanagement hat das Ziel, „das(s) Eintreten sicherheitsrelevanten menschlichen Versagens innerhalb des Lebenszyklus weiter (zu) reduzieren und auf diese Weise das Restrisiko sicherheitsrelevanter systematischer Fehler (zu) minimieren“ [DIN EN 50129].

Der vierte Teil (Technischer Sicherheitsbericht) ist der zentrale Teil des Sicherheitsnachweises. Dort werden das zu entwickelnde System und seine Komponenten, welche ihrerseits als Teilsysteme verstanden werden können, bezüglich

ihrer Sicherheit basierend auf der entsprechend den Anforderungen aufgebauten Systemarchitektur beschrieben. Weiterhin wird der Nachweis der funktionalen, technischen und betrieblichen Sicherheit des Systems erbracht. Die Fehlerraten der Komponenten können zugeteilt werden. Die Systemarchitektur und die Sicherheitsprinzipien sind graphisch und verbal darzustellen. Der geplante betriebliche Einsatz des Systems sollte inklusive der geplanten Geschwindigkeit skizziert werden, wobei externe Einflüsse berücksichtigt werden. Dabei wird der Verweis auf die klimatischen Bedingungen des Betriebs vorgenommen und möglicherweise eine resultierende Einschränkung bezüglich des geographischen/ klimatischen Einsatzes vorgenommen. Die Funktionalität von Soft- und Hardware sowie die korrekte Systemfunktion und Testabläufe sind weitere Teile des technischen Sicherheitsberichts. Zudem ist der Nachweis des korrekten funktionalen Verhaltens, Ausfallauswirkungen, Betrieb mit externen Einflüssen, sicherheitsbezogene Anwendungsbedingungen sowie eine Sicherheitserprobung zu dokumentieren. Ein Verweis zu existierenden Systemarchitekturen und Spezifikationen ist dabei möglich, um die funktionale Sicherheit nachzuweisen. Im technischen Sicherheitsbericht sind ggf. Abweichungen von den anerkannten Regeln der Technik anzugeben und der Nachweis der mindestens gleichen Sicherheit zu erbringen. Weiterhin sind Maßnahmen zu ergreifen und zu dokumentieren, die einen unautorisierten Zugriff auf das System von außen abwenden.

Die Beziehungen zu anderen Sicherheitsnachweisen bildet der fünfte Teil des Sicherheitsnachweises. In diesem wird auf andere Sicherheitsnachweise verwiesen, auf welches sich das zu entwickelnde System oder Teile dessen beziehen. Dies kann bspw. ein Gerät oder ein sicherer Rechner sein. Dort ist die erneute Begutachtung genutzter Sicherheitsnachweise ist nicht notwendig, die relevanten Passagen sind zu betrachten und zu referenzieren. Der Verweis auf andere Nachweise ist für eine beschleunigte und effiziente Nachweisführung empfehlenswert [Schnieder/Schnieder 2013].

Im sechsten, abschließenden Teil des Sicherheitsnachweises werden die genutzten Nachweise vorangegangener Entwicklungen zusammengefasst sowie bestätigt, dass das System durch Entsprechung mit den maßgebenden gesetzlichen Grundlagen alle Sicherheitsbedingungen erfüllt.

Durch die Struktur und das damit verbundene Vorgehen wird nachgewiesen, dass Gefährdungen mit Hilfe geeigneter Prozesse identifiziert wurden und praktikable Maßnahmen zur Schadensminderung und zum Umgang mit Risiken, die von den identifizierten Gefährdungen ausgehen, eingeführt wurden. Weiterhin müssen anwendungsspezifische Kontrollmechanismen definiert, angepasst und praktikabel implementierbar sein.

3.3.4 Einfluss der TSI auf Entwicklung und Zertifizierung

Als Grundlage für die Interoperabilität zwischen den Eisenbahnen Europas wurden von der EU klare Verantwortlichkeiten bezüglich der Begutachtung von Schienenfahrzeugen und verbundener Komponenten sowie der darauf folgenden Inbetriebnahme festgelegt [EU/2008/57]. Diese Regelungen sind teilweise direkt europaweit gültig, teilweise werden sie mit nationalen Besonderheiten in nationales Recht umgesetzt. Die daraus resultierenden Prozesse stellen für alle Beteiligte Neuland dar und befinden sich im Zusammenspiel von Industrie, Behörden, Ministerien und Prüforganisationen im steten Verbesserungsprozess. In der darauf aufbauenden Empfehlung [EU/2014/897] wurden die Regelungen konkretisiert. Zusätzlich ist zu beachten, dass die Inbetriebnahme von Schienenfahrzeugen und deren Teilen strikt von deren Instandhaltung zu trennen ist. Sowohl die Prozesse als auch die ausführenden Stellen sind verschieden [EU/2011/217].

Auch nach den Vorgaben der TSI wird der Entwicklungsprozess federführend vom Hersteller mit Unterstützung von unabhängigen Experten durchgeführt, auch wird die Unabhängigkeit des Gutachters in den TSI gefordert. Zusätzlich sind aufgrund spezifischer Anforderungen und der Nutzung oder Herstellung des Systems der Betreiber, die Sicherheitsbehörde, der Lieferant, der Hersteller sowie weitere eventuell beteiligte Prüfstellen am sicherheitsgerichteten Entwicklungsprozess beteiligt.

3.3.5 Sicherheitsnachweis im Schienenverkehr weltweit

Aufgrund der geplanten internationalen Anwendung der Ergebnisse dieser Arbeit wird neben der oben aufgeführten Struktur des Sicherheitsnachweises entsprechend europäischer Normierung auch der Sicherheitsnachweis außerhalb Europas betrachtet. Dabei werden starke Unterschiede deutlich, so sind bspw. die Sicherheitsanforderungen für den Personenverkehr in Nordamerika nicht normiert, sie werden von jedem EVU separat festgelegt [Elkins/Carter 1993; Boileau 2014], lediglich im Güterverkehr existieren allgemeine Sicherheitsanforderungen. Der in Nordamerika gewählte Ansatz basiert auf der Definition sicherheitsrelevanter Anforderungen in Bezug auf die Leistungsfähigkeit des Fahrzeugs, die anhand von spezifischen Kriterien zusammen mit den Bedingungen, unter denen diese erreicht werden, gemessen werden. Im Vergleich dazu kann der entsprechend [DIN EN 50126], [DIN EN 50128] und [DIN EN 50129] in Europa gültige Ansatz als pragmatischer betrachtet werden, mit dem ein vielfältiger grenzüberschreitender Verkehr von Zügen realisiert werden kann. In Europa sind Anforderungen entstanden, die praktische Erfahrungen widerspiegeln und weniger analytisch aufgebaut sind [Balliet 2011].

In Nordamerika werden bspw. Tests zur Entgleisungssicherheit auf bestimmten Streckenabschnitten, die eine bestimmte Geometrie aufweisen, durchgeführt. In Europa wird eine Kombination aus Analysen und Tests verwendet [Boileau 2014]. In einem weiteren Beispiel wird deutlich, dass der Nachweis von Sicherheit verschieden aufgefasst wird. So existieren in Europa Grenzwerte für dynamische Kräfte, welche auf die Schienen wirken dürfen, in Nordamerika ist das nicht der Fall, lediglich die Achslast ist begrenzt. In Europa wird der Nachweis über analytische Berechnungen und Schienentests geführt [Balliet 2011]. Speziell im Hinblick auf die wachsende Bedeutung des Im- und Exports von Schienenfahrzeugen erscheint eine Harmonisierung von Sicherheitsgrundlagen im Bahnbereich von Bedeutung, wofür diese Arbeit als Grundlage dienen soll. Ein Überblick über international genutzte Normen ist in Tabelle 3-1 dargestellt.

Tabelle 3-1: International genutzte Normen im Schienenverkehr und ihre Verwendung

Norm	Titel	Geltungsbereich	Verwendung
EN 50129:2003	Bahnanwendungen – Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme – Sicherheitsrelevante elektronische Systeme für Signaltechnik	Europa	Europa, USA
EN 50155:2001	Elektronische Einrichtungen auf Bahnfahrzeugen	Europa	Europa, USA
EN 50159:2011	Bahnanwendungen – Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme – Sicherheitsrelevante Kommunikation in Übertragungssystemen	Europa	Europa, USA
IEC 61508	Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme	Weltweit	USA
IEC 62278:2002	Railway applications – Specification and demonstration of reliability, availability, maintainability and safety (RAMS) (entsprechend EN 50126)	Weltweit	USA Europa (als EN 50126)
IEC 62279:2015	Railway applications – Communications, signalling and processing systems – Software for railway control and protection systems (entsprechend EN 50128)	Weltweit	USA Europa (als EN 50128)
IEEE 1474.1:2004	Communications-Based Train Control (CBTC) performance and functional requirements	Weltweit	USA
IEEE 1483:2000	Verification of Vital Functions in Processor-Based Systems Used in Rail Transit Control	Weltweit	USA
MIL-STD 882E	System Safety	USA	USA

3.3.6 Domänenübergreifender Ansatz

Der in [Leveson 2011] eingeführte domänenübergreifende Ansatz zur Erhöhung der Sicherheit eines technischen Systems führt den Nachweis der Sicherheit über den Versuch des Nachweises dessen Unsicherheit. Damit sei ein aussagekräftiger Sicherheitsnachweis möglich – wenn nicht nachgewiesen werden kann, dass ein System nicht sicher ist, kann davon ausgegangen werden, dass es sicher ist [Leveson 2011]. Mit dieser Herangehensweise aus einer komplementären Perspektive können mögliche Fehler der Designingenieure aufgedeckt werden. Bei der Aufgabe, die Sicherheit eines Systems

nachzuweisen, wird sich darauf konzentriert, Beweise so zu interpretieren, dass das gesteckte Ziel erreicht wird. Wenn das Ziel jedoch der Nachweis der Unsicherheit eines Systems ist, wird angenommen, dass eine andere Herangehensweise gewählt wird [Dekker 2006], was zu einem Sicherheitsgewinn führen kann.

3.3.7 Strukturierung der Sicherheitsnachweisführung

Aufgrund der Komplexität der den Sicherheitsnachweisen zugrunde liegenden Normen sind vielfältige Unterstützungen durch Methoden und Software verfügbar. So verfolgt die durch die Universität York entwickelte Methode der Goal Structuring Notation (GSN) das Ziel, den Nachweis der Sicherheit strukturiert zu führen [Kelly/Weaver 2004]. Mit einem eingerichteten Dokumentenmanagementsystem wird der Forderung von nationalen Sicherheitsbehörden und unabhängigen Sicherheitsprüfern nach einem effizienten Nachweisprogramm nachgekommen [von Buxhoeveden/Trog 2012]. Zusammen mit [DIN EN 50126], [DIN EN 50128] und [DIN EN 50129] wird eine effizientere und kostengünstigere Nachweisführung ermöglicht.

Die GSN zeigt, wie sich Sicherheitsziele in Sicherheitsanforderungen herunterbrechen lassen und mit Lösungen belegbar sind. Dabei werden die eingesetzten Strategien sowie die verwendeten Annahmen begründet erläutert [von Buxhoeveden/Trog 2012]. Das Hauptziel ist dabei immer der Nachweis der Sicherheit eines Systems, wofür wiederum Unterziele definiert und erfüllt werden müssen. Bei Nutzung von Strategien, die unter den Umgebungsbedingungen relevant sind, kann jedem Subziel eine Lösung in Form eines Dokuments oder Nachweises zugeordnet werden [von Buxhoeveden/Trog 2012]. Diese Subziele können auch normative Sicherheitsanforderungen aus der Norm sein.

Eine softwareseitige Unterstützung der Sicherheitsnachweisführung bietet weiterhin das Tool „CATS“ (CodeAnalyzerToolSet). Dieses ermöglicht eine effiziente Verarbeitung der in den Normen dargestellten Anforderungen [Phadrus Systems 2013].

3.3.8 Zusammenfassung der Ansätze

Aus den Beispielen des Sicherheitsnachweises in verschiedenen Domänen wird deutlich, dass die Struktur des Sicherheitsnachweises auf die Domänen abgestimmt ist, wobei die Grundideen, wie in Abbildung 3-6 deutlich wird, vergleichbar sind. Daraus wird eine in der Darstellung hervorgehobene allgemeine Struktur entwickelt. Diese fasst die Aspekte der analysierten Konzepte der Sicherheitsnachweisführung zusammen und ist somit domänenübergreifend und im Schienenverkehr anwendbar.

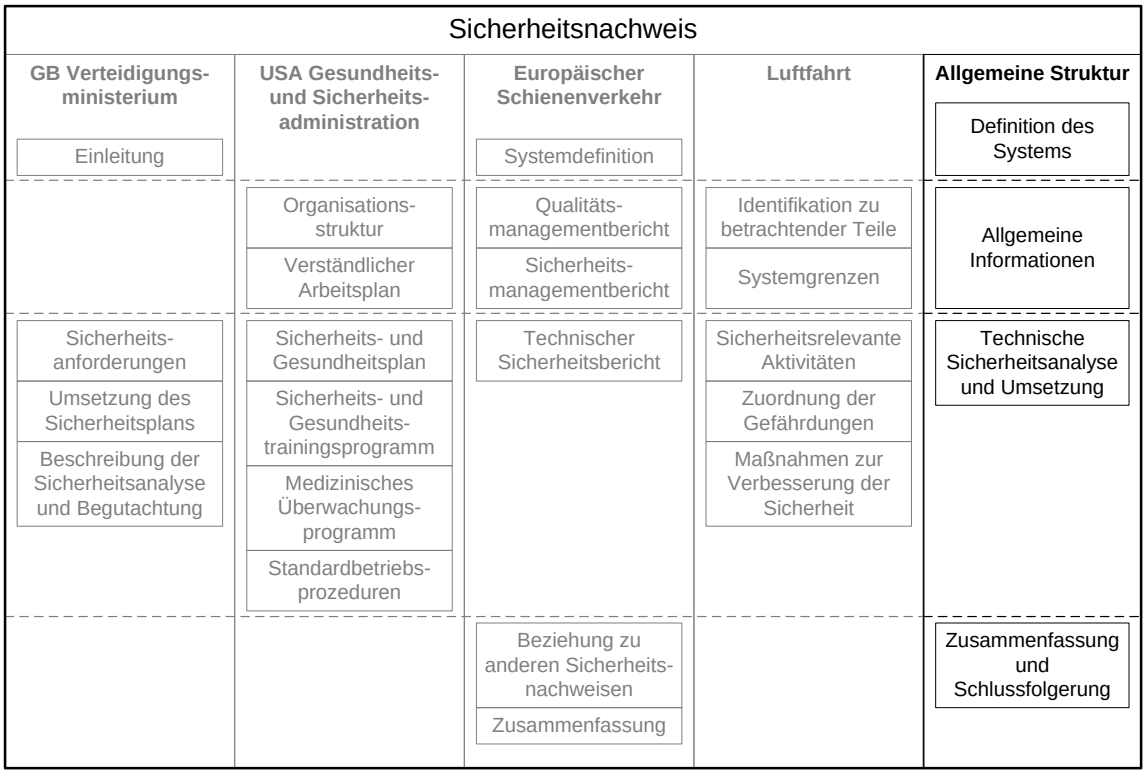


Abbildung 3-6: Struktur des Sicherheitsnachweises in verschiedenen Domänen [Edwards 2000; DIN EN 50129; Maguire 2006]

3.4 Normative Anforderungen im Schienenverkehr

In diesem Abschnitt werden die Anforderungen aus den normativen Dokumenten für die Beteiligten (Betreiber, Halter und Instandhalter) an ein interoperables System im Schienenverkehr extrahiert. Dieser Schritt birgt insbesondere für kleine Betreiber Schwierigkeiten bezüglich der Auswertung und Einhaltung der an sie gestellten normativen Anforderungen an einheitliche Sicherheitsstandards. Das wird dadurch verstärkt, dass die Nichtrelevanz bestimmter normativer Anforderungen zu bewerten und begründet zu dokumentieren ist [Rösch 2012]. Eine Vielzahl an Leitfäden und Erläuterungen macht die bestehenden Regelungen noch unübersichtlicher, weswegen es sinnvoll erscheint, Anforderungskriterien für die Beteiligten modular darzustellen [Rösch 2012].

Die Risikoakzeptanzkriterien von Systemen im Schienenverkehr wird in Abschnitt 3.4.1 betrachtet. In Abschnitt 3.4.2 werden Anforderungen dargestellt, die im Schienenverkehr eingesetzte Komponenten generell erfüllen müssen, was sich größtenteils auf das Verhalten gegenüber externen Einflüssen bezieht. In Abschnitt 3.4.3 werden normative Anforderungen erläutert, die sich auf den Ablauf des Entwicklungsprozesses im europäischen Schienenverkehr beziehen und aus den in Abschnitt 3.2 eingeführten Dokumenten extrahiert wurden. Um von internationalen Vorgehensweisen profitieren zu

können, wird in Abschnitt 3.4.4 ein Blick auf Entwicklungsprozesse in anderen Ländern geworfen, woraus die in Abschnitt 3.4.5 dargestellte Durchführung der sicheren Systementwicklung resultiert, darauf aufbauend wird in Abschnitt 3.4.6 die Nachweiskonzeption entwickelt. In Abschnitt 3.4.7 wird die Notwendigkeit der entwicklungsbegleitenden Dokumentation dargestellt. Abschnitt 3.4.8 beschreibt die für einen Betrieb des Schienenfahrzeugs notwendige Inbetriebnahmegenehmigung.

3.4.1 Risikoakzeptanzkriterien im Schienenverkehr

Die Sicherheit bei technischen Änderungen oder Neuentwicklungen wird bspw. anhand von Risikoakzeptanzkriterien nachgewiesen (Abschnitt 3.1.4). Traditionell wird dabei ALARP (As low as reasonable practicable) vorrangig im Vereinigten Königreich angewandt, GAMAB (Globalement au moins aussi bon) in Frankreich und MEM (Minimale Endogene Mortalität) in Deutschland [DIN EN 50126].

Bei Anwendung von ALARP soll das Risiko eines technischen Systems so gering wie vernünftigerweise praktikabel sein. Risiken werden dabei in drei Kategorien unterteilt – akzeptable Risiken, tolerierbare Risiken (ALARP-Bereich) und nicht akzeptable Risiken. Ein Risiko im akzeptablen Bereich braucht nicht betrachtet werden, tolerierbare Risiken sollten reduziert werden, wenn es mit vertretbarem Aufwand möglich ist. Risiken im nicht akzeptablen Bereich müssen, falls nicht außergewöhnliche Umstände, bspw. bezüglich des finanziellen Aufwands, dagegensprechen, verbessert werden. Diese Unterscheidung kann mit einer Kosten-Nutzen-Analyse getroffen werden [Slovak 2006], wobei Verletzungen und Todesfolgen ein monetärer Wert zugeordnet werden kann.

GAMAB wird als „insgesamt mindestens so gut“ übersetzt. Somit dürfen neue Systeme kein höheres Risiko als vergleichbare Systeme aufweisen [DIN EN 50126]. Diese Vorgehensweise stellt die an der Sicherheitsbetrachtung beteiligten Personen vor die Herausforderung, die Sicherheit eines in Betrieb befindlichen Systems, für welches unter Umständen keine Sicherheitsbetrachtung sondern lediglich Statistiken verfügbar sind, mit der Sicherheit eines im Entwurf befindlichen Systems zu vergleichen. Das Erreichen der mindestens gleichen Sicherheit wird bspw. in der EBO gefordert [EBO 2012], was aufgrund der dadurch steigenden Sicherheit ein Hemmnis für Innovationen sein kann, da für eine immer höhere Sicherheit ein stetig wachsender Entwicklungs- und Nachweisaufwand betrieben werden muss und sich dieser Aufwand unter Umständen nicht rechtfertigen lässt.

Das Prinzip MEM vergleicht das Risiko, welches von technischen Systemen auf einen Menschen einwirkt, mit der natürlichen menschlichen Sterblichkeit. Dieses Risiko

unterscheidet sich entsprechend der betrachteten Altersgruppe, somit wird für eine allgemeine Betrachtung die Altersgruppe mit der geringsten Sterblichkeit (zwischen 5 und 15 Jahren) für einen Vergleich herangezogen [DIN EN 50126]. Je höher die von einem System verursachte Unfallschwere (betroffene/ potentiell getötete Personen) und je mehr technischen Systemen eine Person zu einem Zeitpunkt ausgesetzt sein kann, umso sicherer muss das System sein.

Bei der Betrachtung des Sicherheitsniveaus eines im Schienenverkehr eingesetzten Systems ist zudem zu berücksichtigen, dass das erreichte Niveau bereits hoch ist und eine weitere Erhöhung möglicherweise nur mit unverhältnismäßig hohem Aufwand und somit Kosten möglich ist. Der Fokus sollte sich also darauf richten, die Sicherheit im Schienenverkehr lediglich aufrechtzuerhalten und diese nur zu erhöhen, falls dies mit vertretbarem Aufwand möglich ist [EU/2004/49].

3.4.2 Normative Anforderungen an Komponenten im Schienenverkehr

In diesem Abschnitt werden Anforderungen an Schienenfahrzeuge betrachtet, die aus den in Abschnitt 3.2.3 und Abbildung 3-3 dargestellten Normen resultieren. Dies betrifft bspw. den Temperaturbereich, in dem ein sicherer Betrieb des Fahrzeugs möglich sein muss sowie weitere Umwelteinflüsse. So muss für eine Zertifizierung ein EMV (Elektromagnetische Verträglichkeits)-Plan vorliegen und mit Klassifikationen und Beschreibungen während des Entwicklungsprozesses aktualisiert werden. Weiterhin werden in [DIN EN 50155] Anforderungen bezüglich Spannungsversorgung/ Installation gestellt. Elektronische Einrichtungen müssen verschiedene Versorgungsspannungen unterstützen und Prüfungen durch Spannungsstöße nach [DIN EN 50121-3-2] bestehen. Zur Zuverlässigkeitsbewertung soll das Betriebsverhalten überwacht werden, notwendige und verbotene Wartungsmaßnahmen sind jeweils festzulegen. Zudem muss die Software eine Überwachungsfunktion zur Störungsbehebung enthalten. Weiterhin sind für Komponenten und Techniken, die in Bahnanwendungen nicht erprobt sind, Nachweise zu liefern, dass diese Komponenten oder Techniken den normativen Anforderungen entsprechen [DIN EN 50155]. Dort wird auch eine Anforderung bezüglich der Lebensdauer eines Schienenfahrzeugs gestellt, es soll 24 Stunden pro Tag über 20 bis 30 Jahre betrieben werden können [Heller 2013]. Die identifizierten Anforderungen dieser und weiterer Normen sind in allen Entwicklungen des Schienenverkehrs einzuhalten und nachzuweisen.

3.4.3 Normative Anforderungen an den Entwicklungsprozess

Die Entwicklung eines technischen Systems ist so durchzuführen, dass Gefährdungen vermieden werden und die Funktionen die Anforderungen erfüllen. Für die Begutachtung der Leit- und Sicherungstechnik werden entsprechend den Vorgaben der Sicherheitsbehörde entwicklungsbegleitend Dokumente wie das Lasten- und Pflichtenheft inhaltlich geprüft. So sind zum Nachweis der Sicherheit die Erfüllung des ca. 100 Funktionen umfassenden Technischen Sicherheitsplans Fahrzeug (TeSip), der in die Kategorien Fahren, Bremsen und Fahrzeug unterteilt ist, nachzuweisen [EBA 2012].

Den Funktionen des TeSip sind Sicherheitsanforderungen, Beispiele, Systemgefährdungen sowie Gefährdungseinstufungen zugeordnet. Einige der definierten Systemgefährdungen haben Ortungsbezug und somit eine besondere Relevanz für diese Arbeit [EBA 2012]:

- Fahrzeug setzt sich ungewollt durch Aufschalten von Traktion in Bewegung
- Fahrzeug fährt in falsche Richtung
- Unbemerkt zu hohe Geschwindigkeit
- Ungewollte Zugtrennung

Die Systemgefährdung „ungewollte Zugtrennung“ lässt sich dabei weiterhin entsprechend ihrer Gründe untergliedern – das können ruckartiges Beschleunigen oder Bremsen, automatisches Entkuppeln oder sonstige Ursachen wie bspw. ein mechanischer Schaden sein. Zudem können durch die zur Ortung im Fahrzeug eingebauten technischen Einrichtungen elektrische Wechselwirkungen mit anderen Anlagen und Fahrzeugen verursacht werden. Dies kann eine Störung von externen Anlagen oder eine Störung von sicherheitsrelevanten Funktionen innerhalb des Fahrzeugs durch Störstrahlung bewirken. Während des Entwicklungsprozesses ist zu gewährleisten, dass das Auftreten dieser Störungen vermieden wird, was entsprechend nachzuweisen ist.

Die bisher in Deutschland relevanten Aufgaben und Verantwortlichkeiten für Hersteller, Betreiber und Sicherheitsbehörden halten nicht mit der Innovationsgeschwindigkeit im Bereich der Leit- und Sicherungstechnik Schritt [Leining et al. 2013]. Zudem müssen bestehende Prozesse aufgrund der oben erwähnten Änderung der TSI angepasst werden, weiterhin ist eine Verlagerung von Aufgaben und Verantwortungen notwendig.

Bei der Entwicklung innovativer, moderner Systeme stehen unter Umständen anerkannte Regeln der Technik nicht zur Verfügung oder können nicht angewandt werden. In solchen Fällen ist die Anwendung eines sicherheitsgerichteten Ermessenspielraums notwendig [VV NTZ ÜGR Stufe 2 2013]. Dafür wird ein Projektteam gebildet und ein

Systemgutachter beauftragt. Die Sicherheitsbehörde ist mittels einer Anzeige über die angestrebte Entwicklung zu informieren, welche mit Hilfe eines Prüfplans durchgeführt wird. Um derartige, individuelle Entwicklungen nur selten durchführen zu müssen, ist die Erstellung zusätzlicher anerkannter Regeln der Technik angestrebt.

In Abbildung 3-7 wird ein möglicher iterativer Ablauf der Erarbeitung eines Lastenheftes dargestellt, was Grundlage für die Durchführung des Entwicklungsprozesses ist. Der Konformitätsnachweis ist dabei zu relevanten Teilen der TSI Schienenfahrzeuge zu erstellen. Eine bereits vorliegende Risikoanalyse wird ergänzt, in der Gefährdungsanalyse werden Anforderungen aus der Risikoanalyse nachgewiesen. Als neuer Aspekt wird die Möglichkeit von Ermessensentscheidungen hinzugefügt. Die Begutachtung nach jedem einzelnen Schritt wird durch den Gesamtgutachter durchgeführt.

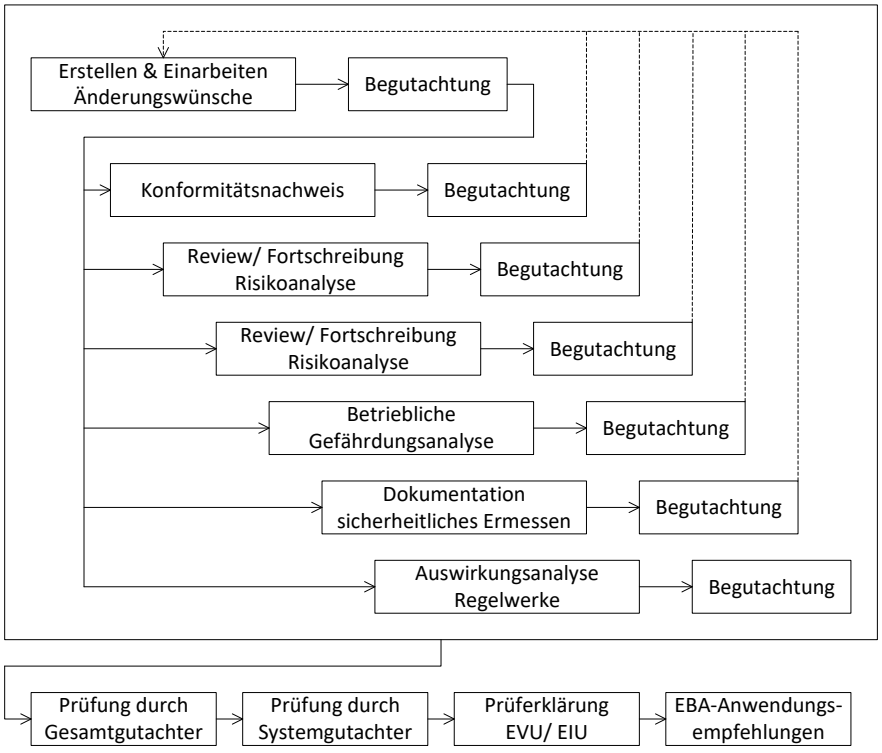


Abbildung 3-7: Elemente zur Erarbeitung des Lastenhefts [Leining et al. 2013]

3.4.4 Normative Anforderungen an den Entwicklungsprozess (international)

Vor Einführung einheitlicher Regelungen existierten neben den verschiedenen Entwicklungsprozessen in Europa internationale Ansätze, die zur Nutzung von Synergien in dieser Arbeit hier kurz eingeführt werden.

In den USA hat die FRA als Teil des Department of Transportation (DOT) den sicheren, verlässlichen und effizienten Transport von Passagieren und Gütern zu überwachen [FRA

2014]. Bevor ein System in Betrieb genommen wird, muss die zuständige Eisenbahngesellschaft einen Sicherheitsplan bei der FRA vorlegen, um eine Systemzulassung zu erhalten. Dieser kann sich auf eine vorliegende Typzulassung beziehen, wenn der Zulieferer zertifiziert ist. Im Sicherheitsplan muss nachgewiesen werden, dass das System nach dessen Vorgaben hergestellt wurde und das beschriebene Sicherheitsniveau erreicht wurde [Petrek 2010]. Er muss von einer unabhängigen Instanz begutachtet werden, um die Umsetzung der Sicherheitsanforderungen unabhängig zu bewerten. Bei Ersatz eines bestehenden Systems durch ein neues System ist der Nachweis mindestens gleicher Sicherheit zu erbringen [FRA 2010].

An das im Entwicklungsprozess zu erstellende Gutachten werden Anforderungen gestellt, bspw. sollen Schwächen und potenziell gefährliche Betriebszustände, nicht vollständige oder abgelehnte Dokumente, angewandte Regelwerke sowie genutzte Methoden dargestellt werden [FRA 2010]. Zur Durchführung der geforderten Tests muss eine vollständige Systembeschreibung vorliegen und das Betriebskonzept sowie der Testablauf einschließlich notwendiger Schutzmaßnahmen beschrieben sein [FRA 2010]. Weitere Tests können behördlich angeordnet werden.

In Russland bildet das dortige technische Reglement [TR TS 001/2011] die normative Grundlage der Sicherungssysteme von Schienenfahrzeugen. Zugbeeinflussungssysteme müssen bspw. unter den dortigen klimatischen und mechanischen Bedingungen betrieben werden können und dürfen keine elektromechanischen Störungen verursachen. Gefährliche Zustände durch Bedienfehler sollen ausgeschlossen werden. Die Ausrüstung der Triebköpfe im Hochgeschwindigkeitsverkehr mit satellitenbasierter Ortung ist genau wie eine On-Board-Diagnose, ein Informationsaustauschsystem zur Leitstelle sowie einer Wachsamkeitsprüfung des Triebfahrzeugführers mit Zwangsbremsung vorgeschrieben [TR TS 002/2011]. Um die fünf Jahre gültige Zertifizierung zu erhalten, müssen technische Dokumente, der Sicherheitsnachweis, Testprotokolle, eine Übersicht der verwendeten Normen sowie die Zertifizierung des Managements vorgelegt werden. Die Verlängerung der Zertifizierung um ein Jahr ist möglich, wenn keine Änderungen vorgenommen wurden und keine Kundenbeschwerden vorliegen.

Aus dieser Betrachtung wird deutlich, dass auch international die Entwicklung auf Normen aufbaut, um ein strukturiertes Vorgehen sicherzustellen. In den USA werden, vergleichbar zu Europa, ein Sicherheitsplan, eine Begutachtung sowie das Einhalten mindestens gleicher Sicherheit vorgeschrieben. In Russland werden Innovationen durch gesetzliche Vorgaben vorangetrieben.

3.4.5 Durchführung der sicheren Systementwicklung

Die sichere Systementwicklung kann klassisch durch eine Entwicklung gemäß der in der CENELEC Normung vorgegebenen Prozessschritte oder innovativ durch eine sichere Systemmodellierung entsprechend des STAMP Ansatzes nach [Leveson 2012] durchgeführt werden. Durch die weitreichenden Erfahrungen mit dem CENELEC Ansatz sind für diesen detaillierte Anweisungen und Prozesse zur Durchführung der Nachweisführung verfügbar, die trotz des innovativen Charakters genutzt werden können. Die innovative Anpassung des Entwicklungsprozesses an die Integration von Industriekomponenten in den Schienenverkehr ist sicherlich wünschenswert, wird hier jedoch aufgrund der vagen Möglichkeit der Umsetzung nicht betrachtet.

Die GSN, die bspw. von EUROCONTROL für die sicherheitsgerichtete Darstellung bevorzugt wird [Fowler 2005], ist ein weiteres geeignetes Hilfsmittel, da sie die Strukturierung der in einem Entwicklungsprozess genutzten und erstellten Dokumente ermöglicht und somit eine gute Basis für eine strukturierte Entwicklung und Nachweisführung bildet. Bei Änderungen in einem Dokument ist die Nachverfolgung der daraus folgenden notwendigen Änderungen möglich. Zudem werden den zertifizierungsrelevanten Dokumenten dem Hauptziel untergeordnete Subziele zugeordnet. Deren Einhaltung soll durch die Gewährleistung der sicheren Funktionalität der einzelnen Funktionen sichergestellt werden. Dies kann bspw. durch die im Rahmen einer Fehlermöglichkeits- und -einflussanalyse (Failure Mode and Effects Analysis – FMEA) extrahierten potenziellen Fehler des Systems erfolgen [May 2010]. Die GSN oder der STAMP Ansatz ermöglichen dabei eine Rückverfolgung und somit eine gewisse Vollständigkeit. Dies entspricht auch dem Ansatz aus [Defence Standard 00-56], in dem der Sicherheitsnachweis aus einer Reihe von Behauptungen besteht, die nachgewiesen werden müssen.

Zu Beginn des sicherheitsgerichteten Entwicklungsprozesses ist ein Sicherheitsziel anzugeben, falls dies nicht geschieht muss das Sicherheitsziel aus der Systemarchitektur abgeleitet werden. Eine frühzeitige Kommunikation mit allen Beteiligten, insbesondere mit der Sicherheitsbehörde inklusive der notwendigen Antragstellung, kann zu einer Beschleunigung der Zertifizierung beitragen. Die Behörde und Gutachter sollten jederzeit die Möglichkeit haben, interne Kontrollen und Audits durchzuführen.

Die Sicherheitsanforderungen werden bei der Erstellung der Entwurfsprinzipien und den zugehörigen Berechnungen, bei den Testspezifikationen und -ergebnissen sowie bei der Sicherheitsanalyse und den Sicherheitsergebnissen berücksichtigt. Zum entsprechenden Nachweis ist das betriebliche Risiko zu ermitteln, was durch eine Sicherheitsanalyse erfolgen kann [Slovak 2006]. Unter Nutzung des strukturierten Systems kann zum

Nachweis der Sicherheit der einzelnen Komponenten eine Gefährdungsanalyse bspw. mit einer FMEA durchgeführt werden [Klinge 1998]. Die FMEA kann sich dabei auf die Datenauswertung der durch die Sensoren gelieferten Informationen [May 2010] oder der einzelnen Funktionen des betrachteten Systems fokussieren. Dafür müssen die Ausfallraten der einzelnen Komponenten entsprechend den Bedingungen des gültigen normativen Rahmens bekannt sein oder berechnet werden können und nach Veränderungen aktualisiert werden. Bei einer FMEA werden unerwünschte Ereignisse definiert und deren mögliche Ursachen mit einer Eintrittswahrscheinlichkeit dargestellt [Slovak 2006]. Zudem werden jeweils Risikoeinschätzung, Maßnahmen, Schweregrad und Konsequenzen des Auftretens betrachtet. Diese können bewertet werden, um zu empfehlende Maßnahmen abzuleiten [May 2010]. Die Bewertung der Sicherheitsrelevanz erfolgt über eine Risikoprioritätszahl (RPZ). Bei Inkludierung der Risikobeurteilung und somit einer subjektiven Einschätzung kann von einer Fehlermöglichkeits-, -kritizitäts- und -einflussanalyse (Failure Mode, Effects, and Criticality Analysis – FMECA) gesprochen werden [May 2010].

3.4.6 Nachweiskonzeption

In diesem Abschnitt wird als Grundlage für den Entwicklungsprozess eine Struktur der zu erzeugenden Dokumente erstellt, um zu gewährleisten, dass die Systementwicklung vollständig durchgeführt wird, wofür Anpassungen der normativ vorgegebenen Struktur entsprechend den Erkenntnissen der vorherigen Abschnitte vorgenommen werden. Dies ist notwendig, da in der normativen Struktur alle wesentlichen Informationen als Inhalte für den technischen Sicherheitsbericht als Teil des Sicherheitsnachweises gefordert sind und sich damit nicht an der Reihenfolge der sinnvollerweise durchzuführenden Bearbeitung orientieren. So sind bspw. im Kapitel 5 des technischen Sicherheitsberichts sicherheitsbezogene Anwendungsbedingungen zu definieren. Darin werden Regeln, Bedingungen und Einschränkungen erstellt, die bei der Anwendung des Systems eingehalten werden müssen, um die Sicherheit zu gewährleisten. Diese während Betriebs- und Instandhaltungsprozessen einzuhaltenden Bedingungen sind einerseits sinnvoll, um den Betrieb eines bestehenden Systems zu ermöglichen, anderseits müssen diese Bedingungen permanent beachtet und somit geschult werden, was den Betrieb des Systems durch den damit verbundenen Aufwand erschwert. Daher sollten im Systementwurf frühzeitig Lösungen gefunden werden, um die Anzahl der zu erstellenden Anwendungsbedingungen zu reduzieren. Grundsätzlich ist es zweckmäßig, Anforderungen an Betrieb und Instandhaltung (4.5.2[3]) in den Anforderungsspezifikationen, Anforderungen an Stilllegung und Entsorgung (4.5.4[3]) in

[3] Abschnitt im technischen Sicherheitsbericht nach [DIN EN 50129]

den Anforderungs- und Sicherheitsanforderungsspezifikationen sowie Anforderungen an Sicherheitsüberwachung im Betrieb (4.5.3[3]) in den Sicherheitsanforderungsspezifikationen zu berücksichtigen. Zudem erscheint die Zuordnung der Anforderungen an die Sicherheitserprobung (4.6.1[3]) zu den Sicherheitsanforderungsspezifikationen sinnvoll.

Um im Dokument „Definitionen des Systems“ als Teil des Sicherheitsnachweises bereits einen umfassenden Überblick über das betrachtete System zu geben, werden dort drei Kapitel (Einleitung, Systemarchitektur, sichere Systementwicklung) vorgeschlagen. Im Kapitel Systemarchitektur wird dieses beschrieben (4.2.1[3]) und Schnittstellen definiert (4.2.2[3]). Die Projektierung von Teilsystemen/-einrichtungen und Systemaufbau (4.5.1[3]) erfolgt im dritten Kapitel der Definition des Systems (sichere Systementwicklung) gemeinsam mit der Zusammenfassung der technischen Sicherheitsprinzipien (4.1.2[3]).

Die resultierende Struktur ist in Abbildung 3-8 dargestellt. Für eine Rückverfolgbarkeit sind dort die ursprünglichen, normativen Kapitelnummern und -abschnitte[3] angegeben. Diese Struktur wird im weiteren Verlauf dieser Arbeit als Prozess zur sicheren Systementwicklung und als Vorlage zur zugehörigen Dokumentation genutzt.

In dieser Darstellung wird deutlich, dass mit den Anforderungsspezifikationen und den Sicherheitsanforderungsspezifikationen zunächst die Anforderungen an das System bearbeitet werden, aus denen sich die Spezifikationen (Systemarchitektur als Teil der Definition des Systems des Sicherheitsnachweises) und daraus die Funktionen (sichere Systementwicklung als Teil der Definition des Systems des Sicherheitsnachweises) ableiten lassen. Die dargestellte Struktur ist Grundlage für die folgenden Abschnitte, in denen Anforderungsspezifikationen, Sicherheitsanforderungsspezifikationen, Sicherheitsnachweis und Sicherheitsgutachten betrachtet werden.

Generell kann bei Sicherheitsnachweisen in drei verschiedene Arten, einen generischen Produktsicherheitsnachweis, einen generischen Anwendungssicherheitsnachweis und einen spezifischen Anwendungssicherheitsnachweis unterschieden werden. Diese Struktur sollte jedoch nicht zu starr fixiert werden, eine Kombination dieser drei Arten ist denkbar und sinnvoll. Eine strikte Unterteilung erschwert möglicherweise die Nachvollziehbarkeit der resultierenden Dokumentation, durch die Zusammenfassung wird eine umfassendere Betrachtung ermöglicht.

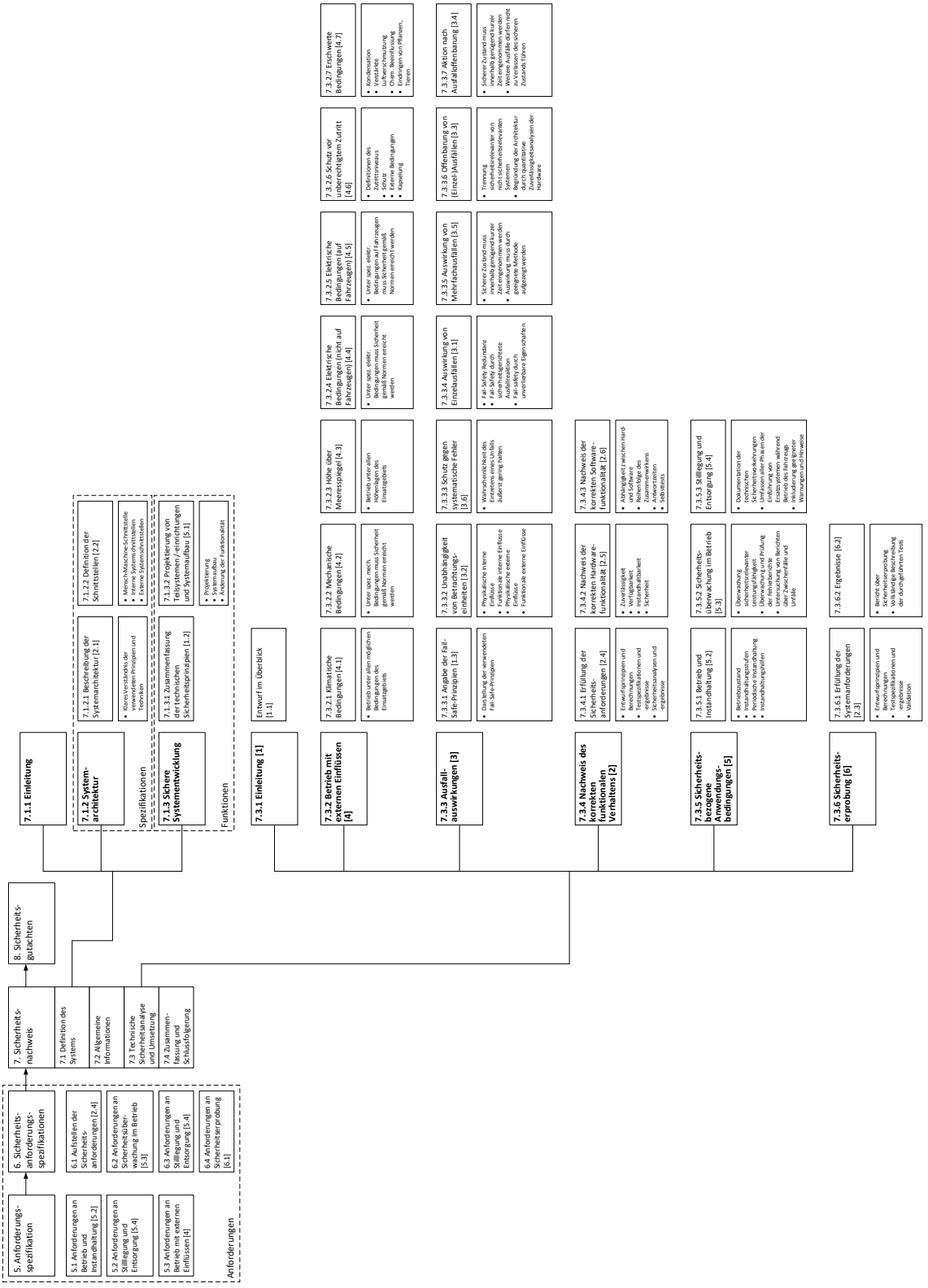


Abbildung 3-8: Vorgeschlagene Struktur der Entwicklung und Dokumentation eines technischen Systems

3.4.7 Normkonforme entwicklungsbegleitende Dokumentation

Für die normkonforme Dokumentation eignen sich zunächst regelmäßige Fortschrittsberichte der Systemarchitektur sowie der Hard- und Softwareentwicklung. Diese Fortschrittberichte sind insbesondere während des Entwicklungsprozesses von Bedeutung, um den Wissensstand der Beteiligten auf einem einheitlichen Niveau zu halten. Die anschauliche Darstellung in Grafiken und erklärenden Tabellen trägt auch für den Gutachter zum Verständnis der durchgeführten Entwicklungsmaßnahmen bei.

Eine normkonforme entwicklungsbegleitende Dokumentation ist ein wesentlicher Bestandteil des Entwicklungsprozesses und eine Grundlage für eine effiziente Sicherheitsnachweisführung. Sie ermöglicht allen Beteiligten ein Systemverständnis des jeweiligen Produkts sowie einen gemeinsamen Wissensstand zur Beurteilung der Systemeigenschaften und zur Vorbereitung des sicheren Betriebs.

Dabei sind Eingangsdokumente normativ vorgegeben, Ausgangsdokumente müssen den normativ vorgegebenen Strukturen entsprechen und werden als Teil des Entwicklungsprozesses mit Verantwortlichkeiten erzeugt. Die Ausgangsdokumente sind wesentlich für die an die Entwicklung anschließende Begutachtung, da sie den Begutachtungsgegenstand darstellen. Die textuellen technischen Spezifikationen sollten mit Skizzen ergänzt werden, da diese das Verständnis bezüglich des Produkts visuell unterstützen und eine Grundlage für die spätere Herstellung bilden. Daher sind detaillierte Pläne technischer Details, bspw. Verdrahtungspläne, einzubeziehen. Die detaillierte Beschreibung der Entwicklung der einzelnen Komponenten ist speziell bei der Integration externer Industriekomponenten notwendig, um diese Dokumente als einen Teil der Sicherheitsnachweisführung zu inkludieren.

In die normkonforme Dokumentation fließen bereits durchgeführte Sicherheitsnachweise von in zu entwickelnden Systemen verwendeten Komponenten ein, eine erneute Begutachtung ist im Normalfall nicht notwendig. Die relevanten Passagen des Sicherheitsnachweises der integrierten Dokumente sind jedoch im Sicherheitsnachweis des zu entwickelnden Produkts zu betrachten und zu referenzieren.

Weiterhin sollten Erweiterungen oder Veränderungen der normativen Grundlagen leicht eingearbeitet werden können, auch können Vorschläge zur Weiterentwicklung des normativen Rahmens ein mögliches Ergebnis sein.

3.4.8 Inbetriebnahmegenehmigung

Die Entwicklung eines Schienenfahrzeugs wird mit der Erteilung der Inbetriebnahmegenehmigung abgeschlossen, ohne die der Betrieb eine Ordnungswidrigkeit [TEIV 2004] wäre. Dessen Beantragung erfolgt durch den Betreiber, den Fahrzeughalter oder den Hersteller in dem Mitgliedsstaat, in dem das Schienenfahrzeug in Verkehr gebracht werden soll [TEIV 2004]. Die Inbetriebnahmegenehmigung kann gleichzeitig als Serienzulassung beantragt werden, was in der Regel der Fall ist, deren Gültigkeit ist auf sieben Jahre beschränkt [EBA 2015]. Dafür sind folgende Dokumente, sofern relevant, vorzulegen [EU/2009/352]:

- Zwischenprüfbescheinigung
- EG-Prüferklärung
- Prüfung anhand nationaler Vorschriften
- Bewertung der CSM
- Teilsystem-Inbetriebnahmegenehmigung
- Erste Inbetriebnahmegenehmigung für Fahrzeuge
- Zusätzliche Inbetriebnahmegenehmigung
- Genehmigung von Fahrzeugtypen

Die Sicherheitsbehörde muss den Antrag binnen vier Monaten bearbeiten [TEIV 2004]. Bei Nichterfüllen grundlegender Anforderungen wie bspw. unzureichender Instandhaltung, Konstruktionsfehlern oder die Funktionen einschränkende Defekte sind entsprechende Maßnahmen zu ergreifen, die bis zu einem Zurückziehen der Inbetriebnahmegenehmigung reichen können.

Die Erteilung der Inbetriebnahmegenehmigung erfolgt basierend auf Abstimmungen zwischen dem EBA und dem Antragsteller auf Basis eines gemeinsam vereinbarten Ablaufplans mit dem Ziel eines schnellen und reibungslosen Ablaufs. Neben den vorzulegenden Dokumenten sind ein Nachweisplan, Termine zur Zwischenabstimmung sowie geplante Zeitpunkte zur Vorlage der Nachweise und Erklärungen sowie der Inbetriebnahmegenehmigung notwendig [BMVBS 2013]. Ein besonderes Augenmerk sollte dabei auf mögliche Änderungen des technischen Regelwerks gelegt werden, es sollte sich auf dessen gemeinsamen Stand verständigt werden. Auch kann der Antragsteller über einen Vorschlag zur Lösung von Regelungslücken Einfluss auf die zukünftige Gestaltung des normativen Rahmens nehmen [EBA 2015]. Nach Erteilung der Inbetriebnahmegenehmigung kann das Schienenfahrzeug sofort eingesetzt werden, bei Vorliegen einer ausländischen Inbetriebnahmegenehmigung gilt dies, sobald der Nachweis erbracht wurde, dass nationale Besonderheiten eingehalten werden.

4 Entwicklung sicherer Systeme und Systemstrukturierung

In diesem Kapitel wird die strukturierte und konsistente Entwicklung eines technischen Systems als Grundlage für die Entwicklung einer satellitenbasierten Ortungseinheit zur sicheren Nutzung im Schienenverkehr betrachtet. Dafür wird in Abschnitt 4.1 die Entwicklung technischer Systeme im Schienenverkehr zunächst generisch betrachtet und in Abschnitt 4.2 eine terminologische Strukturierung des Systembegriffs durchgeführt, um die Entwicklung strukturiert und konsistent durchführen zu können. In Abschnitt 4.3 werden Ansätze zur Systemstrukturierung dargestellt.

4.1 Entwicklung technischer Systeme im Schienenverkehr

Die in Abschnitt 2.4 eingeführte satellitenbasierte Sensorik soll durch die Entwicklung einer Ortungseinheit zur sicheren satellitenbasierten Ortung als Teil eines Zugbeeinflussungssystems nutzbar gemacht werden. Am Anfang der sicheren Entwicklung eines technischen Systems stehen zunächst die aus den betrieblichen Anforderungen resultierenden spezifizierten Funktionen und die Anforderungen an die Sicherheit des Systems. Spezifizierte Funktionen und Sicherheitsanforderungen können konträr sein, da eine gewünschte Funktion auf einem geforderten Sicherheitsniveau schwierig zu erfüllen sein kann. Nach Herbeiführen von Kompromissen zwischen diesen Aspekten sind die korrekten Funktionen bei Ausfallfreiheit zu entwickeln. Auf Basis derer ist, wie in Abbildung 4-1 dargestellt, der Nachweis des korrekten funktionalen Verhaltens zu erbringen.

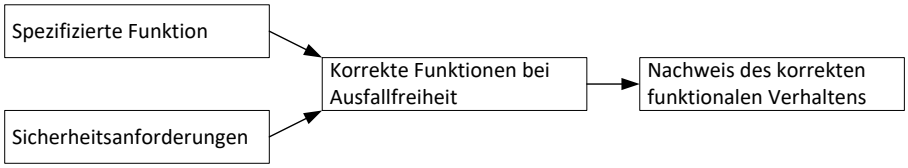


Abbildung 4-1: Prozess der sicheren Systementwicklung

Der generische sicherheitsgerichtete Entwicklungsprozess eines technischen Systems mit Fokus auf den Schienenverkehr wird in Abschnitt 4.1.1 betrachtet. Darauf aufbauend folgen die entsprechenden Verantwortlichkeiten, zunächst domänenunabhängig in Abschnitt 4.1.2. Diese Verantwortlichkeiten unterscheiden sich im Schienenverkehr je nach gewünschter Sicherheitsstufe, weswegen diese in Abschnitt 4.1.3 eingeführt werden. Die Verantwortlichkeiten sind ebenso im Entwicklungsprozess, der in Abschnitt 4.1.4 betrachtet wird, relevant. Dort wird zudem auf die Aufgaben von Sicherheitsbehörden eingegangen, da diese als abschließend prüfende Instanz eine besondere Bedeutung haben. Daran anschließend werden die Verantwortlichkeiten während der Zertifizierung in Abschnitt 4.1.5 betrachtet.

4.1.1 Generischer sicherheitsgerichteter Entwicklungsprozess

Der generische sicherheitsgerichtete Entwicklungsprozess eines technischen Systems beginnt mit der Erstellung der Anforderungen, aus denen die Spezifikationen abgeleitet werden. Anschließend erfolgt die Sicherheitsbetrachtung, welche die Ermittlung der Situationen und Bedingungen, in welchen das System ein unerwünschtes Ereignis hervorrufen kann, beinhaltet [Slovak 2006; Drewes 2009]. Dabei werden die Konsequenzen, Schwere und Wahrscheinlichkeiten charakterisiert, wofür das Betriebskonzept, verfügbare Entwurfsdokumente und bereits identifizierte Gefährdungen genutzt werden. Maßnahmen zur Minderung von Gefährdungen mit einem nicht akzeptablen Risiko müssen definiert werden [Braband 2005].

Generell sind bei einer sicheren Systementwicklung die drei Sicherheitsstrategien Gefährdungsvermeidung, Gefährdungsabwehr und Schadensminderung zu implementieren. Damit soll verhindert werden, dass während der Durchführung des Verkehrsprozesses ein Schaden als unerwünschtes Ereignis eintritt [Drewes 2009; Schnieder et al. 2009b; Schnieder 2010; Schnieder/Schnieder 2013]. Mathematisch wird dieser Zusammenhang als RISIKO, dem Produkt aus (mittlerer) Eintrittswahrscheinlichkeit eines Schadens PD und einer mittleren Schadenshöhe D aufgrund einer Gefährdungssituation [Schnieder 2012] beschrieben.

> „Risiko ist die Wahrscheinlichkeit des Auftretens einer Gefahr, die einen Schaden verursacht und der Schweregrad des Schadens.“ [DIN EN 50126]

Um zu gewährleisten, dass im Entwicklungsprozess alle relevanten Schritte berücksichtigt werden, orientieren sich diese am normativ vorgegebenen V-Modell [DIN EN 50126; IEC 61508; Braband 2006]. Eine graphische Prozessdarstellung verdeutlicht die Prozessobjekte und deren Verknüpfungen [Rumpe 2011], weswegen für die generische Darstellung des Produktlebenszyklus bis zur Inbetriebnahme die Petrinetznotation nach [Petri 1962] gewählt wird und in Abbildung 4-2 dargestellt ist. Die Schritte des V-Modells sind Zustand oder Zustandsübergang, das jeweils fehlende Element wurde ergänzt. Die generische Struktur des Sicherheitsnachweises [DIN EN 50128] (schwarz) ist kombiniert mit dem normativ vorgeschlagenen Produktlebenszyklus im Schienenverkehr [DIN EN 50126] (grau) dargestellt. Die Beteiligten sind wesentlicher Bestandteil dieser Darstellung und werden als Ressourcen dargestellt.

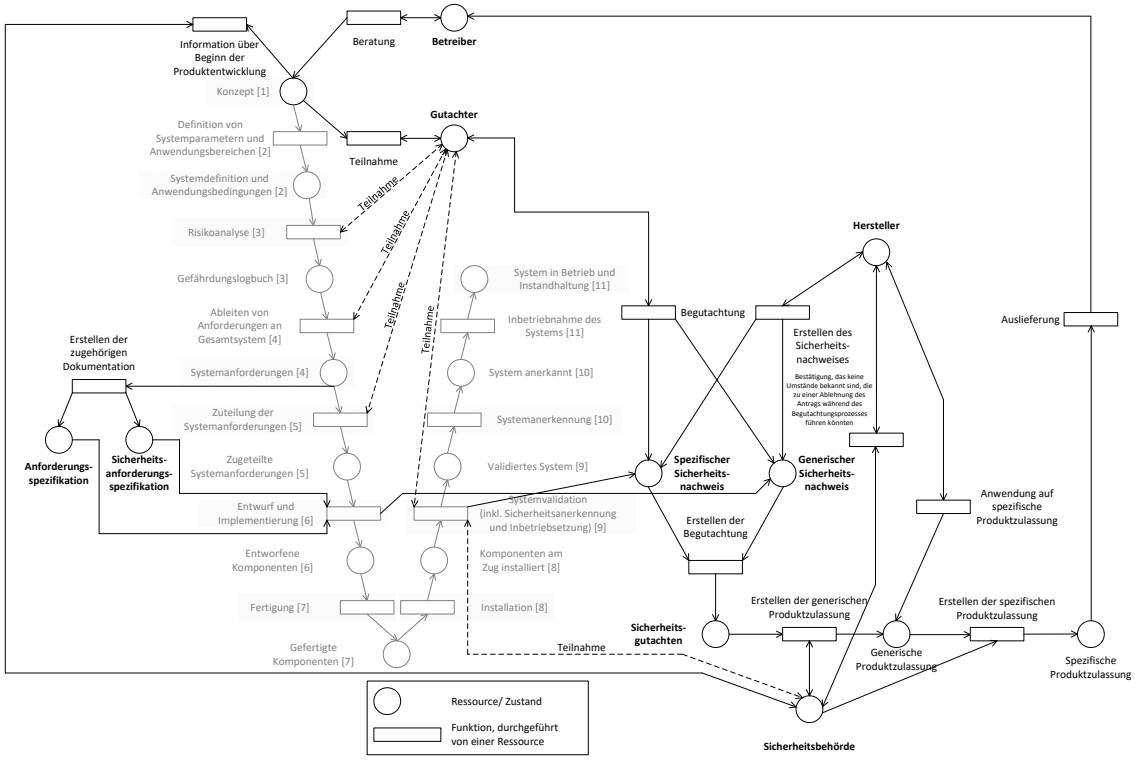


Abbildung 4-2: Entwicklungsprozess mit Lebenszyklus verknüpft [DIN EN 50126; DIN EN 50128]

Durch eine Verifizierung wird die Einhaltung der Spezifikationen überprüft, durch eine Validierung wird überprüft, ob das Produkt entsprechend den Anforderungen entwickelt wurde [DIN EN 50128]. Zusätzlich zu den technischen Maßnahmen kann während der Entwicklung die Sicherheit durch Managementmaßnahmen erhöht werden, was bspw. ein beim Hersteller eingeführtes QMS sein kann. Nach Abschluss der Entwicklung kann die Sicherheit des in Betrieb befindlichen Systems durch betriebliche Maßnahmen wie überprüfende Handlungen des Triebfahrzeugführers erhöht werden. Trotz vielfältig implementierter Sicherungsmaßnahmen ist kein technisches System, Teilsystem oder Bauteil aufgrund seiner physikalischen und chemischen Eigenschaften komplett ausfallsicher und fehlerfrei [DIN EN ISO 12100], eine völlige Gefährdungsfreiheit ist somit nicht möglich [Schnieder/Schnieder 2013], jedoch in der Regel sehr hoch.

4.1.2 Domänenunabhängige Verantwortlichkeiten

Um eine effiziente und zielgerichtete Durchführung des Entwicklungsprozesses zu gewährleisten, sind die normativ festgelegten Zuständigkeiten zu analysieren und zu nutzen. Die Verantwortlichkeiten lassen sich in allen Domänen in der Regel den Institutionen Hersteller, Betreiber, Gutachter und Sicherheitsbehörde zuordnen [DIN EN 50129; GAUSS Basisprojekt 2010]. Der Hersteller ist für die sichere Entwicklung entsprechend den Anforderungen des Betreibers und dem Nachweis der Sicherheit gegenüber Gutachter und Sicherheitsbehörde verantwortlich. Die Sicherheitsbehörde

erteilt die Zertifizierung auf Grundlage der durch den Gutachter durchgeführten Begutachtung der Dokumentation des Herstellers. Der Gutachter muss dabei institutionell unabhängig sein und über ausreichend Fachwissen verfügen.

Die beim Hersteller am Entwicklungsprozess beteiligten Organisationseinheiten lassen sich mit Projektleiter sowie Entwickler-, Erprobungs-, Verifizierungs- und Validierungsteam zusammenfassen. Deren Aufgaben sind in Tabelle 4-1 dargestellt. Organisationseinheit bezeichnet eine oder mehrere Personen, die eine bestimmte Rolle übernehmen, für die eine bestimmte Eignung und Qualifikation notwendig ist. Die Übertragung der Verantwortung an qualifizierte Bevollmächtigte ist möglich, der Besitz der notwendigen Kompetenzen und Qualifikationen ist generell nachzuweisen. Diese Nachweise sind zusammen mit Zertifikaten der Partner, wie zertifiziertes Qualitätsmanagement oder Lieferantenmanagement, im Sicherheitsnachweis zu dokumentieren. Der Sicherheitsbeauftragte ist beim Hersteller für die Überwachung der gesamten sicherheitsrelevanten Prozesse verantwortlich.

Tabelle 4-1: Aufgaben der Institutionen im Entwicklungsprozess nach [Maguire 2006; DIN EN 50128; VV NTZ ÜGR Stufe 2 2013]

Institution	Organisationseinheit	Aufgabe
Projektleiter	Projektleiter	Bereitstellung von Ressourcen, Unabhängigkeit der Rollen Kommunikation inner- und außerhalb des Projekts
Entwicklerteam	Anforderungsmanager	Erstellung von Anforderungen
	Entwerfer	Umsetzung der Anforderungen in Architektur
	Implementierer	Rückverfolgbare Integration der Software auf Zielrechner
	Integrator	Integration der Soft- und Hardware
	Konfigurationsmanager	Freigabe der Softwarekomponenten, Durchführung der Konfiguration
	Sicherheitsingenieur	Implementierung der Sicherheitsaufgaben des Projekts
Erprobungsteam	Tester	Testspezifikationen, Beurteilung der Ergebnisse
Verifizierungsteam[4]	Verifizierer	Lenken des Verifizierungsprozesses inkl. Verifizierungsplans
Validierungsteam[4]	Validierer	Erstellung Validierungsplan mit Gutachter, Überprüfung dessen Durchführung
Begutachtungsteam	Gutachter	Erstellung und Umsetzung eines Begutachtungsplans
Notified Body	Notified Body	Begutachtung
Sicherheitsbehörde	Sicherheitsbehörde	Zertifizierung
Betreiber	Freigabeverantwortlicher	Inbetriebnahme

4.1.3 Personelle und institutionelle Unabhängigkeiten nach Sicherheitsstufe

Im Schienenverkehr sind die normativ geforderten Unabhängigkeiten der involvierten Personen bzw. Rollen und Institutionen entsprechend dem angestrebten Sicherheitslevel verschieden. Je höher das vom System zu erreichende Sicherheitslevel ist, desto höher sind die Anforderungen an System- und Produktentwicklung sowie an personelle und

[4] Validierung und Validation sowie Verifizierung und Verifikation werden teilweise synonym, teilweise zur Unterscheidung verwendet. So wird im Duden als Bedeutung von „Validation“ „Validierung“ angegeben, „Verifizierung“ und „Verifikation“ werden mit „Verifizierung“ beschrieben. In dieser Arbeit wird mit dem Ziel der Unterscheidung Validierung und Verifizierung als Ablauf des Prozesses und Validation und Verifikation als Abschluss des Prozesses betrachtet.

institutionelle Unabhängigkeiten [DIN EN 50129]. Somit steigt entsprechend die Anzahl der beteiligten und voneinander unabhängigen Personen, Rollen und Institutionen, bei geringem Sicherheitslevel kann eine Person oder Institution mehrere Aufgaben übernehmen. Die Zuordnung zu der tolerierbaren Gefährdungsrate pro Stunde ist in Tabelle 4-2 dargestellt.

Tabelle 4-2: Zuordnung von tolerierbarer Gefährdungsrate zu Sicherheitsintegritätsleveln im Schienenverkehr [DIN EN 50129]

Tolerierbare Gefährdungsrate pro Stunde und pro Funktion	Sicherheitsintegritätslevel
$10^{-9} \leq THR < 10^{-8}$	SIL 4
$10^{-8} \leq THR < 10^{-7}$	SIL 3
$10^{-7} \leq THR < 10^{-6}$	SIL 2
$10^{-6} \leq THR < 10^{-5}$	SIL 1
$10^{-5} \leq THR$	SIL 0

Bei einer Zertifizierung mit SIL 0 werden keine sicherheitsrelevanten Funktionen erfüllt, somit ist ein Gutachten lediglich bei einem Einfluss der Sicherheit auf das Gesamtsystem notwendig. Bei Entwicklung eines Produkts, welches SIL 1 bis 4 entsprechen soll, sind personelle und institutionelle Unabhängigkeiten gefordert. Der Gutachter muss für diese SIL eine unabhängige Person sein, welcher einem anderen Unternehmen als dem Entwicklerteam oder einer nicht weisungsbefugten Abteilung angehört. Die entsprechenden Zuordnungen sind in Abbildung 4-3 dargestellt und werden in Abbildung 4-4 angewandt.

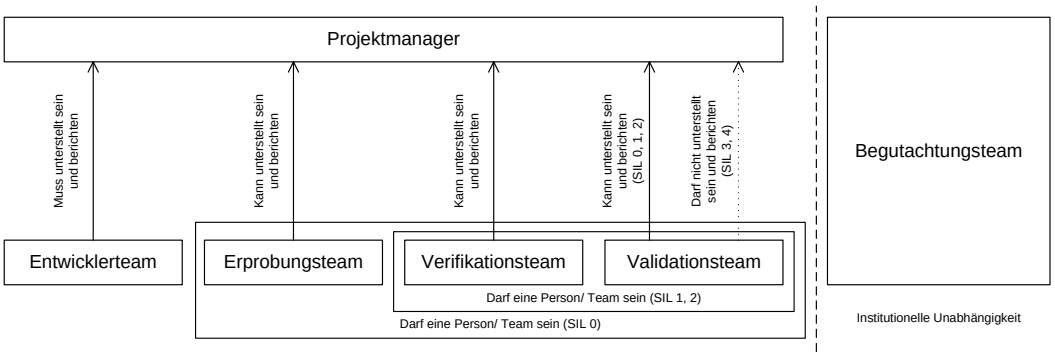


Abbildung 4-3: Normativ festgelegte Organisationsstruktur nach [DIN EN 50128]

4.1.4 Verantwortlichkeiten im Entwicklungsprozess

Zur weiteren Nutzbarkeit wird der Entwicklungsprozess und die damit verknüpfte Zertifizierung nach [Hänsel 2008] entsprechend der notwendigen Prozessschritte und den Verantwortlichkeiten der einzelnen Institutionen gegliedert, dabei wurden Abläufe anderer Domänen berücksichtigt [GAUSS Basisprojekt 2010]. Der vorgeschlagene Entwicklungsprozess, unterteilt nach den Verantwortlichkeiten des Herstellers, Betreibers, Gutachters, der Sicherheitsbehörde und des NoBo, ist in Abbildung 4-4

dargestellt und basiert auf dem zugrunde liegenden normativen Rahmen und dem in Abschnitt 4.1.1 dargestellten generischen sicherheitsgerichteten Entwicklungsprozess.

Zu Beginn des Entwicklungsprozesses, der auf dem normativen Rahmen basiert, werden durch den Betreiber Anforderungen gestellt, die der Hersteller in Spezifikationen, sicherheitsrelevante Details und Systemgrenzen umsetzt. Entwicklungsbezogene Ratschläge des Betreibers erhöhen die Effizienz und reduzieren die Fehlerquote und unterstützen eine schnelle und sichere Produktentwicklung. Bereits hier muss sichergestellt werden, dass die Sicherheitsanforderungen für eine spätere Integration der Ortungseinheit in ein Zugbeeinflussungssystem enthalten sind.

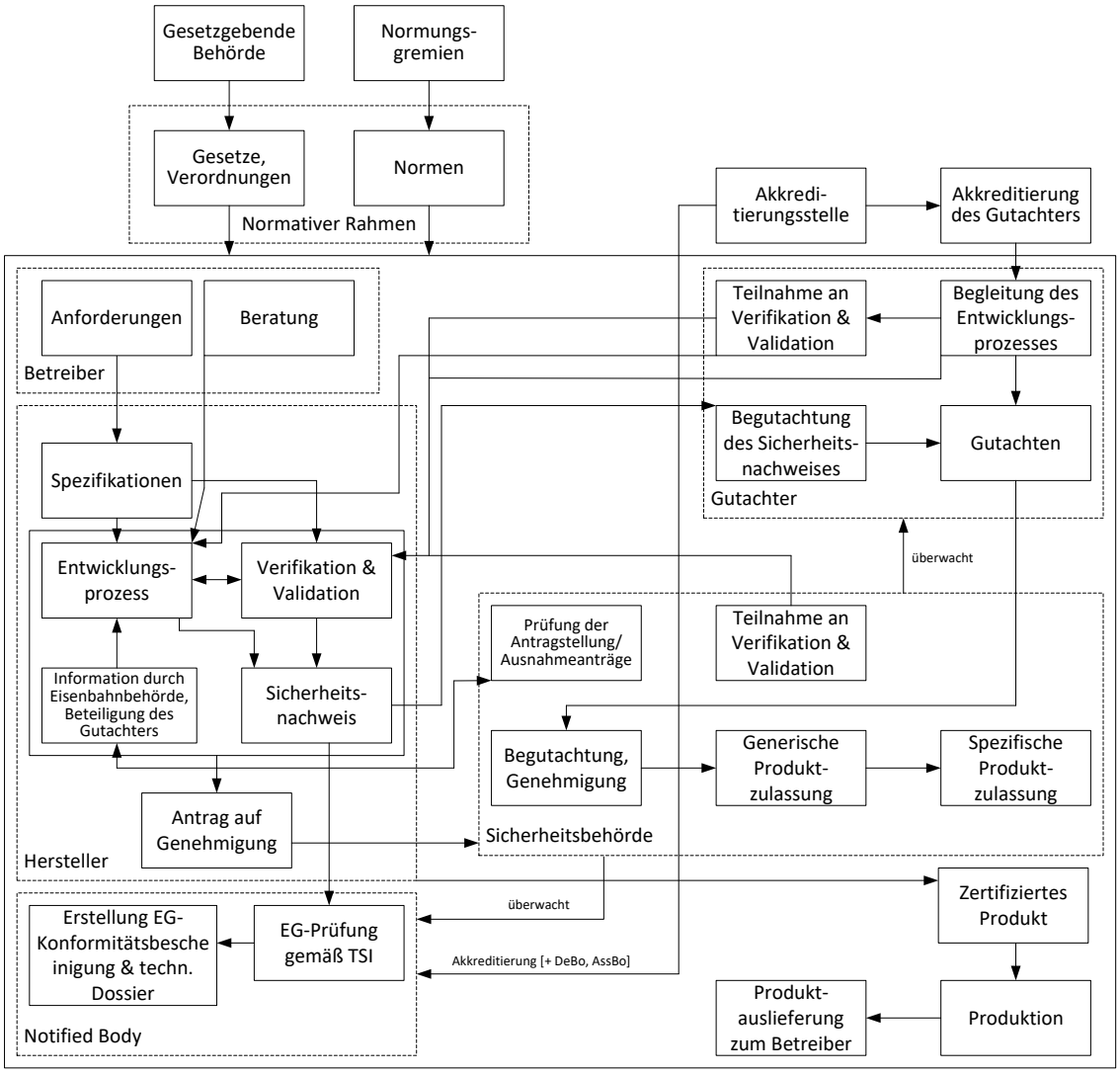


Abbildung 4-4: Entwicklungsprozess und Verantwortlichkeiten nach [Schnieder 2009; GAUSS Basisprojekt 2010; DIN EN 50129]

Der Entwicklungsprozess wird durch eine permanente Verifizierung und Validierung mit dem Ziel einer effizienten Systementwicklung begleitet. Die Einbindung der Sicherheitsbehörde durch Information über den Beginn des Entwicklungsprozesses

empfiehlt sich, um eine Bestätigung zu erhalten, dass keine Umstände bekannt sind, die zu einer Ablehnung des Antrags während der Begutachtung führen könnten. Somit kann verhindert werden, dass die Inbetriebnahme verzögert wird und gewährleistet werden, dass die Zertifizierung in enger Kooperation mit den Sicherheitsbehörden [May 2010] ohne kosten- und zeitintensive Änderungen der Entwicklung durchgeführt wird.

Der Sicherheitsnachweis wird vom Hersteller während des Entwicklungsprozesses erstellt und anschließend beim Gutachter eingereicht, um die Entwicklung entsprechend den Spezifikationen nachzuweisen. Der Gutachter überprüft aufgrund seiner Verifizierung und Validierung während der Entwicklung und seines Wissens die Übereinstimmung des Sicherheitsnachweises mit den normativen Vorgaben. Die gewonnenen Erkenntnisse werden in einem Gutachten zusammengefasst, welches bei der Sicherheitsbehörde eingereicht und dort überprüft wird. Ergebnis einer erfolgreichen Prüfung ist eine generische Produktzulassung. Nach der darauf folgenden, für jede Anwendung separaten, spezifischen Produktzulassung erfolgt die Auslieferung.

Um während der Entwicklung unabhängig von den Änderungen des normativen Rahmens zu sein, kann deren Stand für bis zu sieben Jahre festgeschrieben werden. Innerhalb dieses Zeitraums muss die Serienzulassung erfolgen, im Anschluss ist eine Lieferung des Produkts für weitere sieben Jahre möglich [BMVBS 2011].

4.1.5 Verantwortlichkeiten während der Zertifizierung

Bei der Zertifizierung sind die aktuellen Prüfprozesse und Verantwortlichkeiten entsprechend den TSI zu betrachten [Wiescholek et al. 2015a; Wiescholek et al. 2015b]. In [EU/2011/217] wurde zur Genehmigung der Inbetriebnahme von strukturellen Teilsystemen und Fahrzeugen durch die nationale Sicherheitsbehörde die Dreiteilung in benannte Stelle[5] (BS – Notified Body – NoBo), benannte beauftragte Stelle (BSS – Designated Body – DeBo) und die unabhängige Bewertungsstelle (UBS – Assessment Bodies – AssBo) von der EU vorgegeben, was durch die nationale Gesetzgebung umgesetzt wurde. Zusätzlich existiert eine nationale Sicherheitsbehörde (NSB – National Safety Authority – NSA). Das Fernziel ist, dass diese Organisationen ein in allen Mitgliedsstaaten gültiges europäisches Sicherheitszertifikat ausstellen können [Sciutto et al. 2010]. Die entsprechenden Institutionen, ihre Autorisierungen und Aufgaben sind in Tabelle 4-3 zusammengefasst.

[5] Für NoBo, DeBo, AssBo und NSA werden in dieser Arbeit die englischen Abkürzungen genutzt, da sie wesentlich gebräuchlicher sind.

Tabelle 4-3: Verantwortlichkeiten während der Zertifizierung nach [EU/2011/217; BMVBS 2013; Wiescholek et al. 2015a]

Institution	Autorisierung	Aufgabe
Notified Body (NoBo)	Akkreditiert und überwacht durch NSA	Analyse des zu entwickelnden Systems; Verifizierung der Konformität mit relevanten TSI; Ausstellen der Prüfbescheinigung
Designated Body (DeBo)	Akkreditiert und überwacht durch NSA	Begutachtung der notifizierten nationalen technischen Regeln; Kompetenzen des EBA außer in Kernbereichen (Radsatz, Bremse, Fahrtechnik, Zugsteuerung und Zugsicherung); Muss aus Mitgliedsstaat stammen, in dem Begutachtung stattfindet
Assessment Body (AssBo)	Akkreditiert und überwacht durch NSA	Risikobewertung und Bewertung des Risikomanagementverfahrens nach CSM
Nationale Sicherheitsbehörde (NSA)	Akkreditiert durch nationale Akkreditierungsstelle	Tätigkeit als Eisenbahnaufsicht; fachliche Beteiligung an Entwicklung und Zertifizierung

Der NoBo analysiert und verifiziert die Konformität des entwickelten Systems mit den relevanten TSI entsprechend eines europaweit gültigen Verfahrens zur Überprüfung der EG-Konformität, was mit dem Ausstellen einer Prüfbescheinigung abgeschlossen wird [Eisweiler/Steinebach 2014; TEIV 2004]. Zudem prüft der NoBo die Schnittstellen des zu prüfenden Teilsystems mit dem System, in das es integriert ist oder integriert werden soll [EU/2008/57], was durch die Arbeit von Testlaboren unterstützt werden kann [Sciutto et al. 2010]. Die Akkreditierung der benannten Stellen wird in den Mitgliedsstaaten unterschiedlich gehandhabt, in Frankreich und Deutschland hat eine staatliche Einrichtung diese Funktion, in den Niederlanden oder im Vereinigten Königreich sind mehrere private Institutionen als benannte Stelle akkreditiert.

Aktuell existieren 59 NoBos [EC 2015], die zu einer gegenseitigen Überprüfung zusätzlich zur staatlichen Kontrolle angehalten sind [TEIV 2004]. Damit soll eine vergleichbare Bewertung der Komponenten und eine einheitliche Auslegung der Interoperabilitätsrichtlinien sichergestellt werden [Eisenbahn-Cert 2015].

Der DeBo wurde im Rahmen der Neuordnung der TSI geschaffen. Seine Zuständigkeit ist die Begutachtung der NNTR im Entwicklungsprozess. Er muss daher aus dem Mitgliedsstaat stammen, in dem die Entwicklung stattfindet. Die Anerkennung des DeBo erfolgt durch die NSA, in Deutschland also vom EBA. Mit Umsetzung der europäischen Regeln durch ein Memorandum of Understanding überträgt das EBA seine Prüfkompetenzen – außer in vier Kernbereichen (Radsatz, Bremse, Fahrtechnik, Zugsteuerung und Zugsicherung) – an Interims-DeBos [BMVBS 2013].

Die Rollen des NoBo und des DeBo können von einer Prüforganisation übernommen werden, jedoch müssen die Rollen institutionell voneinander getrennt werden. Für die Bewertung der Risikomanagementverfahren und -bewertung auf Grundlage der CSM ist der AssBo zuständig, der diese in Übereinstimmung mit den legislativen Anforderungen bescheinigt [EU/2013/402]. Es existiert keine minimale oder maximale Anzahl von AssBos in einem Mitgliedsstaat.

Die NSA bringt durch ihre Tätigkeit als Eisenbahnaufsicht Anforderungen in den Entwicklungsprozess ein. Für eine fachliche Beteiligung ist dafür deren Kenntnis und Verständnis des normativen Rahmens und der zum Anwendungsgebiet gehörenden Technik, des Problembereichs, der Randbedingungen, der Hardware, des Betriebssystems und der Schnittstellensysteme sowie analytisches Denkvermögen und eine gute Beobachtungsgabe notwendig. In Deutschland ist diese Behörde seit 1994 das EBA, welches dem BMVI unterstellt ist. Eine bedeutende Aufgabe des EBA ist dabei „die Erteilung und Widerrufung von Betriebsgenehmigungen für Systeme und Teilsysteme“ [Schnieder/Schnieder 2013].

Die Ergebnisse der durch NoBo, DeBo und AssBo durchgeführten Bewertungen sowie die resultierenden technischen Eigenschaften, Bestimmungen und Verfahren des SMS laufen in der NSA zusammen und werden von dieser überwacht. Dabei ist die Berücksichtigung von Erfahrungswerten von großer Bedeutung [Leining et al. 2013]. Die NSA stellt auf Basis der durch NoBo, DeBo und AssBo nachgewiesenen sicheren Integration und technischen Kompatibilität die Inbetriebnahmegenehmigung aus und kann in besonderen Fällen als unabhängige Bewertungsstelle tätig werden. Solche Fälle sind bspw. wesentliche Änderungen in Bezug auf die TSI oder notwendige Interventionen. Dies soll eine doppelte Arbeit von NSA und AssBo verhindern.

4.2 Grundlagen der Strukturierung eines technischen Systems

Für die Erstellung eines Sicherheitsnachweises ist eine Systembeschreibung und eine Abgrenzung des Systems notwendig, weswegen in diesem Abschnitt die Strukturierung eines technischen Systems betrachtet wird. Die Definition des Systems in Abschnitt 4.2.2 stellt, wie in Abschnitt 4.2.1 beschrieben, eine Herausforderung dar, da dieser Begriff in unterschiedlichen Fachgebieten vielfältig mit unterschiedlichen Bedeutungen und damit unpräzise genutzt wird [Schnieder/Schnieder 2010]. Speziell im Schienenverkehr ist es trotz einer Vielzahl zur Verfügung stehender Beschreibungsmittel, Methoden und Werkzeuge noch nicht gelungen, sich auf eine Darstellungsform eines Systems festzulegen, so dass in diversen Normen verschiedene Definitionen existieren [Bepperling 2008]. Um diese Ambiguität zu beseitigen, werden hier allgemein gültige Normen mit Bezug zum Schienenverkehr genutzt, was durch die Forderung der europäischen Gesetzgebung nach einer Strukturierung des Schienenverkehrssystems zur Gewährleistung der Interoperabilität [EU/2011/217] unterstützt wird. Auch europäische Projekte wie INTEGRAIL haben dieses Ziel in Bezug auf ETCS und ERTMS unterstützt [Wullerstorff 2010].

In Abschnitt 4.2.3 werden anschließend die Eigenschaften des Systembegriffs als Basis für eine strukturierte Entwicklung betrachtet und darauf aufbauend die Konzeption der Systemarchitektur beschrieben. Bedeutende Aspekte der Erstellung der Systemarchitektur werden in Abschnitt 4.2.4 dargestellt.

4.2.1 Herausforderungen der Systemstrukturierung

Die Herausforderung bei der Strukturierung eines technischen Systems besteht in einem generischen aber dennoch im Schienenverkehr anwendbaren Vorgehen. In [ERA-REC-02-2007-SAF 2007] – dem Vorgängerdokument der heutigen [EU/2013/402] – wird bspw. gefordert, dass eine Systemstrukturierung folgende Punkte enthalten soll:

- Systemziele, Systemgrenzen, Systemfunktionen, Komponenten, Schnittstellen
- Definition der Systemumgebung (z. B. elektromagnetische Beeinträchtigungen)
- Bestehende Sicherheitsmaßnahmen und Sicherheitsanforderungen
- Bedingungen, welche die Grenzen der Risikobeurteilung bestimmen

Zusätzlich wird in [Bepperling 2008] eine generische, einfache, vollständige, widerspruchsfreie und angemessene Systembeschreibung gefordert. Als Teil der sicheren Systementwicklung wird der Begriff Verlässlichkeit (RAMS) als „zusammenfassende Bezeichnung zur Beschreibung der Zuverlässigkeit und der Sicherheit“ [Müller 2015] eines Systems eingeführt. Somit ist die Zuverlässigkeit eine zusammenfassende Bezeichnung der Überlebensfähigkeit, Instandhaltbarkeit, Instandhaltungsvorbereitungsfähigkeit und Verfügbarkeit [Müller 2015] und durch ein System zu gewährleisten [Schnieder/Schnieder 2013]. Im Fokus dieser Arbeit steht dabei insbesondere die Integration industrieller Komponenten in den Entwicklungsprozess des Schienenverkehrs.

4.2.2 Grundlegende Definitionen

Ein System ist die „Gesamtheit miteinander in Verbindung stehender Objekte“ [DIN EN 81346-1], die eine Zielsetzung, bspw. die Ausführung einer Funktion, haben. Die normativen Anmerkungen, dass ein SYSTEM von anderen Systemen klar abgegrenzt sein soll und hinsichtlich seiner Zielsetzung, bspw. bezüglich der Ausführung einer Funktion, definiert sein soll, werden in [Schnieder/Schnieder 2010] berücksichtigt.

> Ein System ist eine Einheit, die „als solches erkennbar ist und in der Lage ist, sich gegen äußere Einflüsse dauerhaft zu erhalten und aus sich heraus bestimmte Zwecke zu erfüllen.“ [Schnieder/Schnieder 2010]

Zur Strukturierung bietet sich die Nutzung einer Abstraktionshierarchie an, also die Unterteilung in Eigenschaften, Merkmale, Größen, Werte und Einheiten, mit der ein System in eine „Menge von Teilen, die ihrerseits wieder in eine Anzahl in wechselseitiger Beziehung stehender Unterteile zerlegt werden können“ [Schnieder/Schnieder 2010], gegliedert werden kann. Jedes einem System zugeordnete Detail besitzt wiederum eine bestimmte Komplexität und kann somit selbst als System bezeichnet werden, woraus sich ein Geflecht aus unter- und übergeordneten Systemen ergibt [Schnieder/Schnieder 2010]. Diese können als OBJEKTE bezeichnet werden.

> Ein Objekt ist eine „Betrachtungseinheit, die in einem Prozess der Entwicklung, Realisierung, Betrieb, [sic] und Entsorgung behandelt wird.“ [DIN EN 81346-1]

4.2.3 Eigenschaften des Systembegriffs

Die Komplexität des Systembegriffs macht dessen detaillierte Betrachtung notwendig, was mit dem Ziel der terminologischen Präzisierung mittels der Attributhierarchie durchgeführt wird [Schnieder/Schnieder 2010]. Dabei können bspw. Relationen und Inhaltsattribute dargestellt werden, wofür dem Systembegriff die vier abstrakten Eigenschaften „Zustand“, „Funktion“, „Struktur“ und „Verhalten“ zugeordnet werden. Die Eigenschaft Funktion wird zusätzlich in „Speichern“, „Verarbeiten“ und „Übertragen“ gegliedert [Schnieder/Schnieder 2010]. Aus dieser Zuordnung ergibt sich ein erster Ansatz zur Systemstrukturierung. Den Eigenschaften „Zustand“ kann bspw. der Zweckbezug und „Verhalten“ eine mathematische Beschreibung [Schnieder/Schnieder 2010] zugeordnet werden, was in Abbildung 4-5 dargestellt ist.

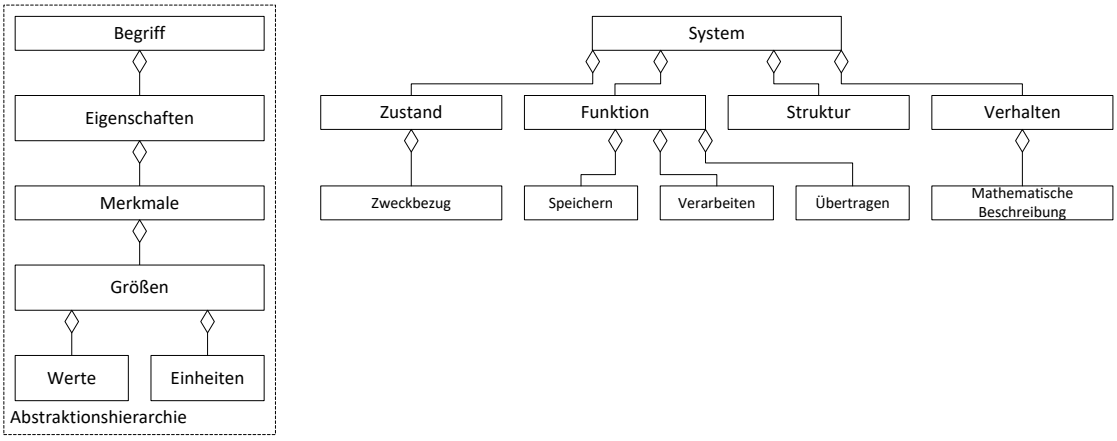


Abbildung 4-5: Nutzung der Abstraktionshierarchie zur Systemdarstellung nach [Schnieder/Schnieder 2010]

Die Systemdefinition hat die funktionalen und betrieblichen Anforderungen als Eingang und bspw. die Systemfunktionen und -grenzen als Ausgang. Parallel dazu wird die

Gefährdungsidentifikation durchgeführt, deren Ausgang sicherheitsrelevante Funktionen und Komponenten sind [Slovak 2006]. Im Rahmen der Systemdefinition werden alle erdenklichen Maßnahmen unternommen, damit gefährliche Betriebssituationen nicht eintreten, wobei immer der schlechteste mögliche Fall betrachtet werden sollte. Im Fokus steht dabei immer die korrekte Funktionalität des Zugbeeinflussungssystems, damit unerwünschte Betriebsereignisse nicht eintreten. Die Gefährdungsidentifikation hat dabei die Aufgabe Komponenten zu identifizieren, die zu einem Gefährdungszustand von Funktionen führen können. Das kann empirisch, also durch Checklisten oder eine FMEA erfolgen oder auch kreativ durch Brainstorming [Slovak 2006]. Auf Grundlage der Gefährdungsidentifikation ist die Beschreibung des Eisenbahnbetriebs durch eine Modellierung des Eisenbahnprozesses und der Unfallfolgen möglich [Slovak 2006].

4.2.4 Bedeutende Aspekte der Erstellung der Systemarchitektur

Bei der Erstellung der Systemarchitektur und der entsprechenden Systemgrenzen sind die funktionalen und betrieblichen Anforderungen sowie Umwelteinflüsse von Bedeutung. Das zu erstellende System wird durch System-Prozess-Schnittstellen mit anderen Systemen interagieren. Im Rahmen der Erstellung der Systemarchitektur ist zudem eine Gefährdungsbetrachtung durchzuführen, bei der mögliche Unfälle, deren Ursachen und Folgen zu betrachten sind, um bereits entsprechende Maßnahmen in den Entwurf der Architektur einfließen lassen zu können.

4.3 Ansätze zur Durchführung der Systemstrukturierung

Zur Planung, Herstellung, Wartung und zum Betrieb eines Systems ist eine Gliederung in Teile, die weiter untergliedert werden können, sinnvoll und notwendig [DIN EN 81346-1]. Die Anforderungen an eine solche strukturierte Darstellung sind jedoch zu komplex, um nur eine Darstellungsart zu nutzen [Erdmann et al. 1994]. Neben der materiellen Aufbaustruktur ist auch die Funktionsstruktur gleichwertig zu betrachten.

Ein technisches System wird von den Akteuren aus verschiedenen Perspektiven betrachtet. So hat bspw. der Hersteller eine andere Sicht als der Betreiber. Entsprechend empfiehlt [Erdmann et al. 1994] die funktionale Gliederung nach dem Strukturprinzip, dem Dekompositionsprinzip, dem Kausalprinzip und dem Temporalprinzip. Die [DIN EN 81346-1] wurde von diesem Grundgedanken beeinflusst, hat jedoch einen ganzheitlicheren Charakter. Dort wird die Strukturierung eines Systems nach dem Funktions-, Produkt- und Ortsaspekt vorgeschlagen. Diese verschiedenen Perspektiven ermöglichen die ganzheitliche Betrachtung des Systems, um das Ziel dieser Arbeit, die Zertifizierung der satellitenbasierten Ortung im Schienenverkehr, zu unterstützen. Es

lassen sich die physikalischen und funktionalen Eigenschaften eines Systems und darauf aufbauend gewollte und ungewollte Interaktionen zu und von anderen Systemen darstellen. Dies geschieht auf Grundlage der gültigen Normen, die aufgrund ihrer Erstellung von einem breit aufgestellten Expertenkreis ein Abbild der anerkannten Regeln der Technik darstellen.

Die funktionsbezogene Struktur (Abschnitt 4.3.1) fokussiert den Zweck des Systems, wohingegen die produktbezogene Struktur (Abschnitt 4.3.2) das System in physikalische Bestandteile untergliedert, welche die technischen Funktionen realisieren. Die ortsbezogene Struktur (Abschnitt 4.3.3) fokussiert die räumliche Gliederung, bspw. die Einbauorte [DIN EN 81346-1]. Mit der in Abschnitt 4.3.4 dargestellten Verflechtung der Aspekte eines Systems lässt sich der zu erfüllende Prozess beschreiben und für die Entwicklung nutzen. Die separate Modellierung ist zunächst notwendig, nach deren Finalisierung ist ein Wechsel der Aspekte zwischen den Ebenen möglich. Die Kombination der Aspekte erfolgt in Abschnitt 7.1.2.1 zur Erstellung und Beschreibung der Systemarchitektur. Diese Verknüpfung durch Unterscheidung der Komponenten nach ihrer Funktionalität ist auch in [DIN EN 15380-2] vorgesehen.

Im Folgenden werden Klassendiagramme verwendet [Rumpe 2011], dessen wichtigste Relationen in Abbildung 4-6 eingeführt werden. Alle Relationen werden dabei als Assoziation bezeichnet, die wiederum eine Generalisierung, Aggregation oder Komposition darstellen können. Die Generalisierung entspricht einer Beziehung zwischen Ober- und Unterbegriff, eine Aggregation einer Teil-Ganzes-Beziehung. Eine Komposition ist ein Sonderfall der Aggregation, wobei die Existenz des Objekts, welches Teil eines Ganzen ist, von der Existenz des Ganzen abhängt.

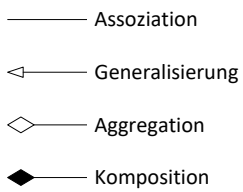


Abbildung 4-6: Übersicht der verwendeten UML-Relationen

4.3.1 Funktionsbezogene Struktur

In diesem Abschnitt wird die FUNKTIONSBEZOGENE STRUKTURIERUNG eines technischen Systems zur späteren Verwendung in dieser Arbeit eingeführt.

> „Eine funktionsbezogene Struktur basiert auf dem Zweck eines Systems. Sie zeigt die Untergliederung eines Systems in Bestandteilobjekte im [sic] Bezug auf den Funktionsaspekt, ohne

dabei mögliche Orts- und/oder Produktaspekte dieser Objekte zu berücksichtigen.“ [DIN EN 81346-1]

Für „Funktion“ existieren verschiedene Definitionen, bspw. in [DIN EN 81346-1], [DIN EN 15380-2] oder in [DIN EN 15380-4] aus [DIN EN IEC 61226]. Gemeinsam legen diese Definitionen ihren Schwerpunkt auf den Zweck, den eine Funktion zu erfüllen hat. In [DIN EN 15380-2] wird ergänzend zu [DIN EN 81346-1] die Betrachtungseinheit in die Definition eingeschlossen, deren Funktion betrachtet wird. In [DIN EN 15380-4] wird zudem das Ziel einer Aufgabe eingeschlossen. Die als Schnittmenge resultierende Definition wird für die Verwendung in dieser Arbeit in Abbildung 4-7, wo der Funktionsaspekt eingeführt wird, dargestellt. Dort wird die „funktionale Gliederungsstruktur“ mit dem Ziel der Zuordnung für Schienenfahrzeuge eingeführt. Die Grundlage der Darstellung bildet [DIN EN 15380-4], deren entsprechenden Funktionsebenen in Klammern angegeben sind. Dabei wird deutlich, dass das „funktionale Einsatzgebiet“, die „Hauptfunktion“, die „Unterfunktion“, die „auf die Aufgabe bezogene Funktion“ und die „auf die Aktivität bezogene Funktion“ auf untergeordneten Ebenen Bestandteile der „funktionalen Gliederungsstruktur“ sind. Alle Ebenen beschreiben dabei selbst Funktionen.

Die Darstellung in Abbildung 4-7 wird genutzt, um den Funktionen Ressourcen allokieren zu können, wobei eine Funktion einer oder mehreren Ressourcen oder eine oder mehrere Teilnehmer einer Ressource zugeordnet werden können. Die Partitionierung bezeichnet die Zuordnung von Funktionen oder Gruppen von Funktionen zu ein oder mehreren Ressourcen und umfasst dabei funktionale, räumliche und technologische Aspekte. Die Allokation kann genau wie die Partitionierung statisch vor Inbetriebnahme oder dynamisch während des Betriebs erfolgen.

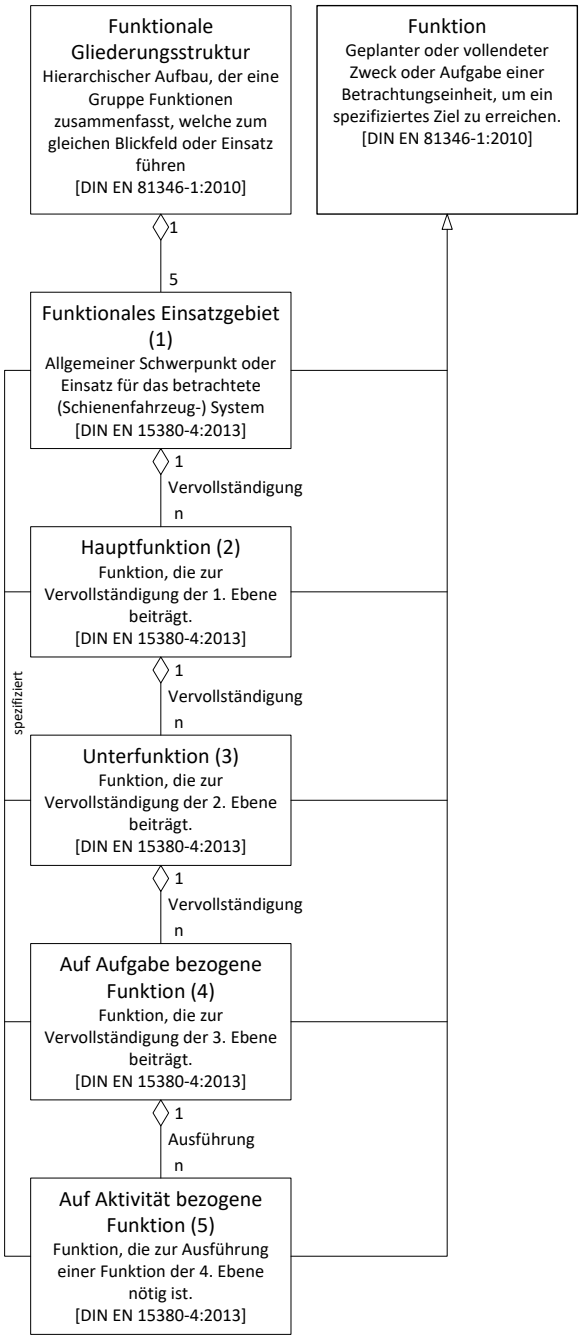


Abbildung 4-7: Funktionsaspekt nach [DIN EN 15380-2; DIN EN 81346-1; DIN EN 15380-4]

4.3.2 Produktbezogene Struktur

In diesem Abschnitt wird die PRODUKTBEZOGENE STRUKTUR eingeführt und in Abbildung 4-8 dargestellt. Dabei können alle als Standardprodukt oder Sonderanfertigung lieferbaren Einheiten als Produkt bezeichnet werden.

„Eine produktbezogene Struktur basiert auf der Art und Weise, wie ein System realisiert, aufgebaut oder geliefert wird, wobei Zwischenkomponenten oder endgültige Komponenten verwendet werden. Eine produktbezogene Struktur zeigt die Untergliederung eines Systems in Bestandteilobjekte im

Hinblick auf den Produktaspekt, ohne mögliche Funktions- und/oder Ortsaspekte dieser Objekte zu berücksichtigen.“ [DIN EN 81346-1]

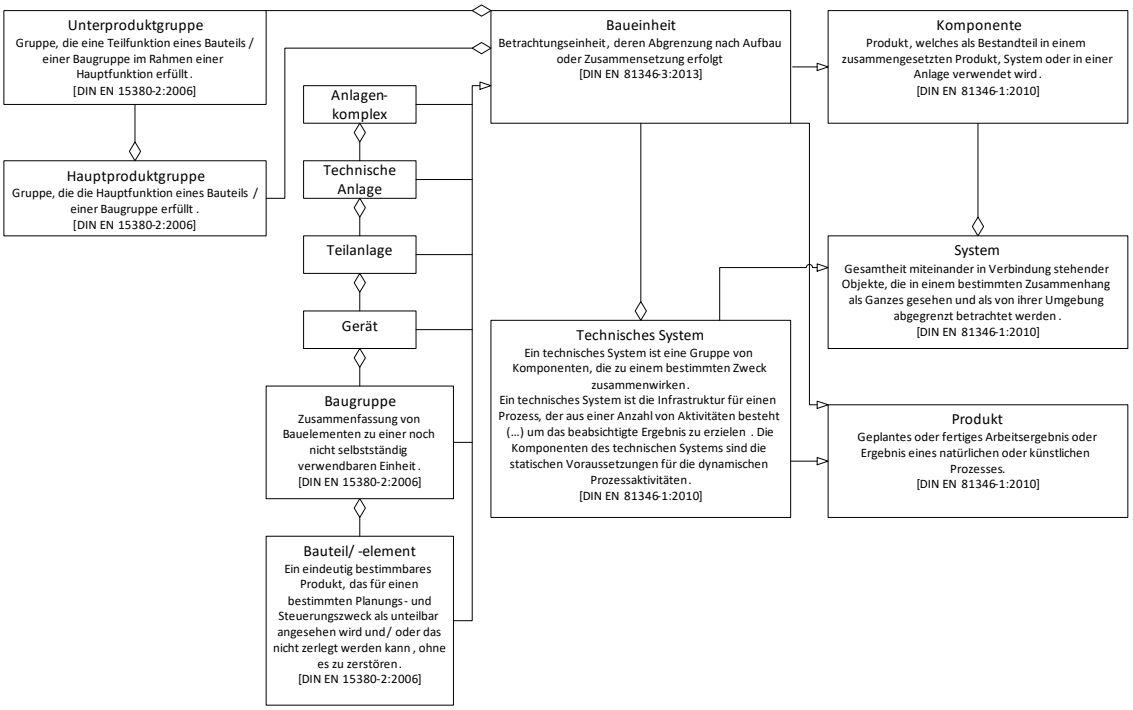


Abbildung 4-8: Produktaspekt nach [DIN EN 15380-2; DIN EN 81346-1]

Aus der in Abbildung 4-8 erfolgten Darstellung wird deutlich, dass ein technisches System als vollständig zusammengebaut betrachtet wird. Es kann aus separat gelieferten Komponenten bestehen. Das technische System wird als Objekt betrachtet, die Komponenten somit als Teilobjekte [DIN EN 81346-1]. Entsprechend der normierenden Zuordnung kann das technische System als System oder Produkt verstanden werden, ihm werden verschiedenartige Baueinheiten zugeordnet. Die Baueinheiten selbst sind wiederum untergliedert, was eine strukturierte Darstellung des Systems ermöglicht.

4.3.3 Ortsbezogene Struktur

Nach der funktions- und produktbezogenen Struktur wird in diesem Abschnitt die ORTSBEZOGENE STRUKTUR betrachtet und in Abbildung 4-9 dargestellt.

„Eine ortsbezogene Struktur basiert auf den räumlichen Bestandteilen eines Objekts oder, falls ausreichend, auf der topographischen Auslegung eines Objekts. Eine ortsbezogene Struktur zeigt die Untergliederung eines Systems in Bestandteilobjekte im Hinblick auf den Ortsaspekt, ohne mögliche Produkt- oder Funktionsaspekte dieser Objekte zu berücksichtigen.“ [DIN EN 81346-1]

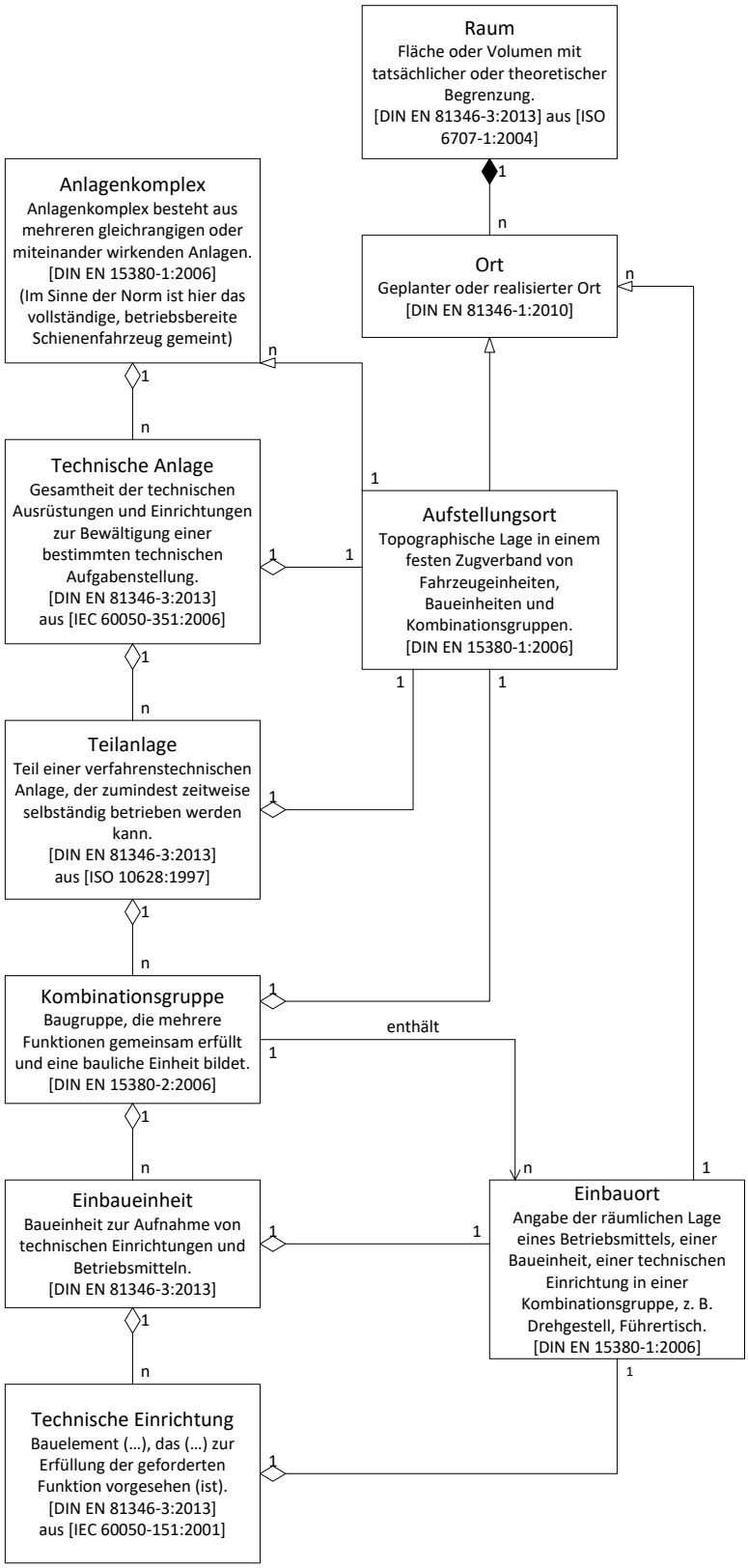


Abbildung 4-9: Ortsaspekt nach [DIN EN 15380-1; DIN ISO 81346-3]

In [DIN EN 81346-1] bezeichnet ein Ort eine Räumlichkeit. Dies kann bspw. der „Einbauplatz (einer Komponente) in einem Montagerahmen in der Struktur einer leittechnischen Einrichtung“ [DIN EN 81346-1] sein.

Der Ortsaspekt, welcher in diesem Abschnitt mit dem Ziel der Strukturierung eines technischen Systems dargestellt wird, bezieht sich dabei auf „definierte Räumlichkeiten innerhalb eines Objekts. Wendet man den Ortsaspekt auf ein Objekt an, ist das Ergebnis dessen interne ortsbezogene Struktur“ [DIN EN 81346-1]. Er ermöglicht zudem die Unterscheidung „innerhalb einer Einbaueinheit sowie die Kennzeichnung von Orten an maschinentechnischen Komponenten und die Kennzeichnung der Orte innerhalb der Anlage“ [DIN EN 15380-2]. Wesentlich dabei ist, dass den technischen Komponenten ein Aufstellungs- und Einbauort zugeordnet wird.

4.3.4 Integrierte Struktur

Durch Nutzung der in Kapitel 3 eingeführten funktions- (Abschnitt 4.3.1), produkt- (Abschnitt 4.3.2) und ortsbezogenen (Abschnitt 4.3.3) Struktur können die Spezifikationen der satellitenbasierten Ortungseinheit aus den funktionalen Anforderungen hergeleitet werden. Dafür wird in Abbildung 4-10 der Funktions- und Produktaspekt verknüpft, um so aus den gewünschten Funktionen die Komponenten des technischen Systems zu konzipieren. Aus den funktionalen Anforderungen als Teil des Funktionsaspekts lassen sich die Systemanforderungen herleiten. Die Verknüpfung zum Ortsaspekt erfolgt über den Einbauort der Baueinheit.

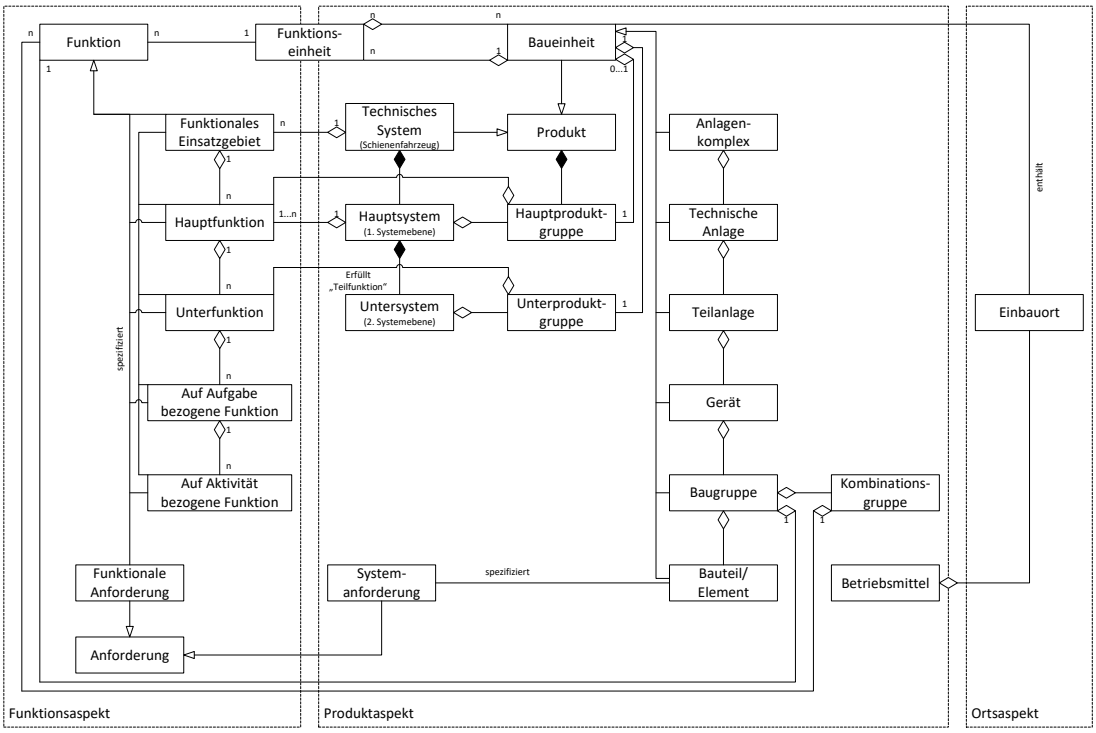


Abbildung 4-10: Kombination des Funktions-, Produkt- und Ortsaspekts

5 Strukturierung der Anforderungsspezifikationen

Anwendungen der satellitenbasierten Ortung im Verkehr haben – abhängig von ihrem Zweck – unterschiedliche Anforderungen an die Ortungsinformation. Durch eine exakte Abstimmung der Ortungsleistung auf die Anforderungen ist die Entwicklung eines technisch optimierten Systems möglich. Dabei sollten nicht mehr Ortungsinformationen als benötigt zur Verfügung gestellt werden, um einen möglichst geringen – auch finanziellen – Aufwand zu betreiben. Ebenso sollten nicht zu wenige Informationen zur Verfügung gestellt werden, um eine optimale Systemfunktionalität zu gewährleisten.

Die Entwicklung eines technischen Systems beginnt mit den Anforderungen, wofür der in Kapitel 2 dargestellte Stand der Technik bezüglich Zugbeeinflussung, Ortung und Sensorik eine wesentliche Basis für die Betriebs- und Einsatzbedingungen bildet. Zudem fließt der in Kapitel 3 dargestellte normative Rahmen sowie die in Kapitel 4 eingeführte sichere Systementwicklung und -strukturierung ein.

Der in diesem und den folgenden Kapiteln 6, 7 und 8 angewandte sicherheitsgerichtete Entwicklungsprozess wurde in den vorherigen Kapiteln erarbeitet. In diesem Kapitel liegt der Fokus auf den Anforderungen an Betrieb und Instandhaltung der Ortungseinheit in Abschnitt 5.1. Abschnitt 5.2 wird zur Beibehaltung der Struktur eingefügt, in Abschnitt 5.3 werden Anforderungen an den Betrieb mit externen Einflüssen betrachtet.

5.1 Anforderungen an Betrieb und Instandhaltung

Wesentlich bei der in diesem Abschnitt durchgeführten Betrachtung der Anforderungen an einen Betrieb der Ortungseinheit ist die Ermittlung der Position des Zuges. Zur Begrenzung des Entwicklungs- und Zertifizierungsaufwands kann das Einsatzgebiet auf bestimmte Streckenkategorien oder ein begrenztes geographisches Gebiet reduziert werden. Der Betrieb soll jederzeit neben den fahrplanmäßig vorgesehenen Zeiten auch nach Betriebsschluss und für Wartungsarbeiten möglich sein. Eine weitere betriebliche Anforderung ist, dass der Start des mit einer Ortungseinheit ausgestatteten Zuges auch nach langer Standzeit möglich sein soll.

5.1.1 Generische Darstellung der Anforderungen an Anwendungen

Ein erster Ansatz zur Darstellung von Anforderungen an Anwendungen der satellitenbasierten Ortung war die Gliederung nach räumlicher Verfügbarkeit, zeitlicher Verfügbarkeit, Sicherheitsrelevanz, horizontaler und vertikaler Genauigkeit sowie Fehlererkennungszeit in einem Diagramm [Poliak 2009], wo jedoch Parametern und

Anwendungen begrenzt darstellbar waren, das daraus resultierende Verbesserungspotential diente als Inspiration für diese Arbeit.

Nach [Meyer zu Hörste/Lemmer 2005] können Anwendungen in Informationsanwendungen und Assistenzanwendungen untergliedert werden – sie sind also rechtlich unbedeutend oder bedeutend. Rechtlich bedeutende Anwendungen sind zudem sicherheitsrelevant oder nicht sicherheitsrelevant. Sicherheitsrelevante Anwendungen sind für den sicheren Verkehrsablauf von besonderer Bedeutung und haben spezielle Anforderungen. Nicht sicherheitsrelevante Anwendungen „haben auch im Falle eines Fehlers keine Auswirkungen auf die Sicherheit von Fahrzeugen, Passagieren oder Umwelt“ [Grimm et al. 2005].

Weiterhin erscheint zur strukturierten Darstellung der Anwendungen die Unterteilung in Verkehrskonstituenten nach [Schnieder 2007] sinnvoll. Daraus wird die in Abbildung 5-1 dargestellte Struktur zur weiteren Anwendung in dieser Arbeit entwickelt, womit den Anwendungen der satellitenbasierten Ortung Funktionen zugeordnet werden können. Dafür werden im folgenden Abschnitt eine Vielzahl von Anwendungen der satellitenbasierten Ortung den vier Verkehrskonstituenten zugeordnet und dort entsprechend ihrer Bedeutung bezüglich Recht und Sicherheit gegliedert.

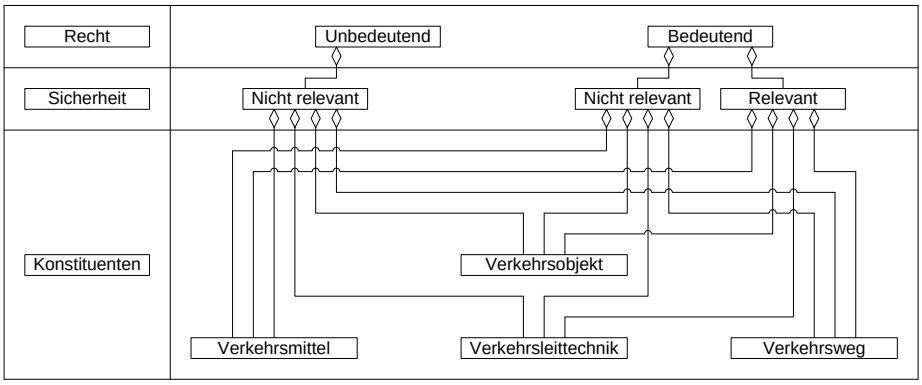


Abbildung 5-1: Struktur der Darstellung der Anwendungen der satellitenbasierten Ortung im Schienenverkehr

5.1.2 Strukturierung der Funktionen im Schienenverkehr

Zunächst werden Anwendungen der Ortung, die der Verkehrskonstituente „Verkehrsobjekt“ zugeordnet werden (Abbildung 5-2), betrachtet. Rechtlich bedeutend ist bspw. die Warnung der Fahrgäste als Verkehrsobjekte vor Zügen sowie eine Alarmierung und ein darauf aufbauender Such- und Rettungseinsatz im Fall von Katastrophen. Die Überwachung von Fracht ist nicht sicherheitsrelevant, wenn sie lediglich logistischen oder dispositiven Zwecken dient, bei gefährlichen Gütern ist sie

sicherheitsrelevant. Weitere Anwendungen sind der Kategorie nicht sicherheitsrelevant und rechtlich unbedeutend zugeordnet.

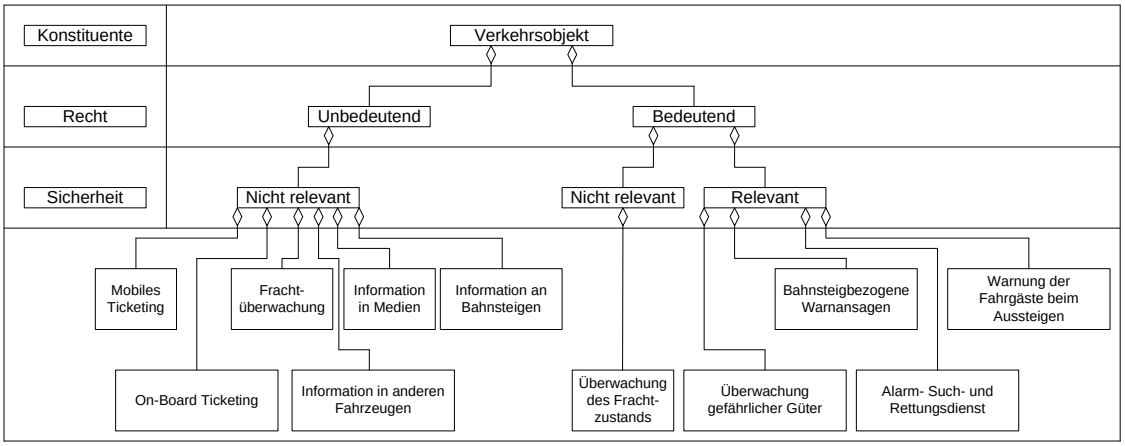


Abbildung 5-2: Anwendungen der Ortung der Kategorie Verkehrsobjekt [Zukunft et al. 2005; Grimm et al. 2005; Strang 2007]

In Abbildung 5-3 werden alle Anwendungen der Ortung, die der Verkehrskonstituente „Verkehrsleittechnik“ zugeordnet werden können, dargestellt. Diese beziehen sich weitestgehend auf die übergeordnete Leitung und Steuerung von Verkehrsobjekten, die sich in Verkehrsmitteln auf der Verkehrswegeinfrastruktur bewegen. Von besonderer Bedeutung sind auch hier sicherheitsrelevante Anwendungen mit rechtlicher Bedeutung. Zudem existieren nicht sicherheitsrelevante und rechtlich bedeutende Anwendungen, die sich mit dem diskriminierungsfreien Zugang zum Schienennetz befassen. Weiterhin existiert eine Vielzahl nicht sicherheitsrelevanter, rechtlich unbedeutender Anwendungen bspw. bezüglich der langfristigen taktischen Planung des Verkehrs.

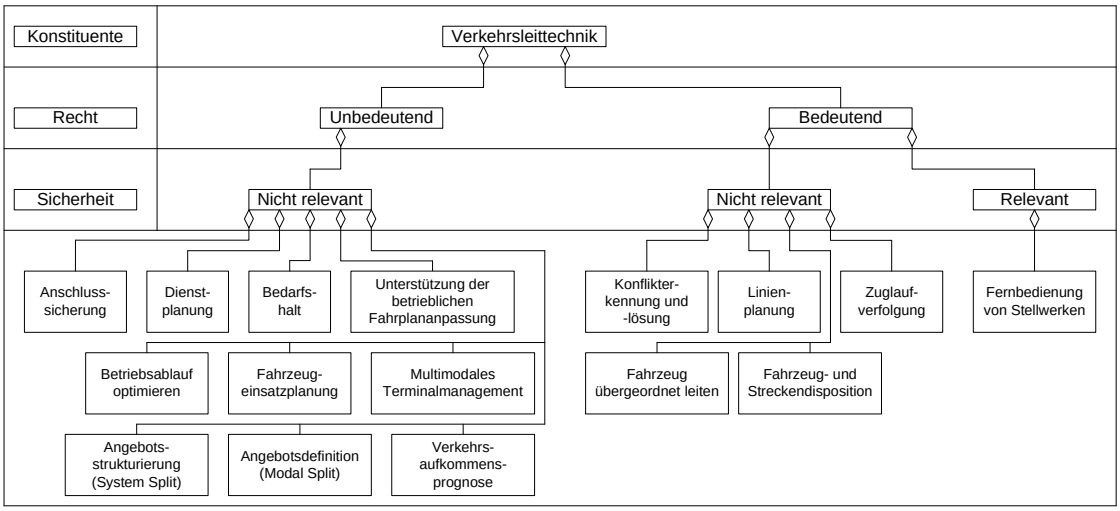


Abbildung 5-3: Anwendungen der Ortung der Kategorie Verkehrsleittechnik [Meyer zu Hörste 2004; Zukunft et al. 2005; Grimm et al. 2005; Strang 2007; EBA 2012]

Die der Verkehrskonstituente „Verkehrsmittel“ zugeordneten Anwendungen der Ortung sind in Abbildung 5-4 zusammengefasst. Dort liegt der Fokus auf sicherheitsrelevanten, rechtlich bedeutenden Anwendungen, größtenteils bezüglich der Zugbeeinflussung.

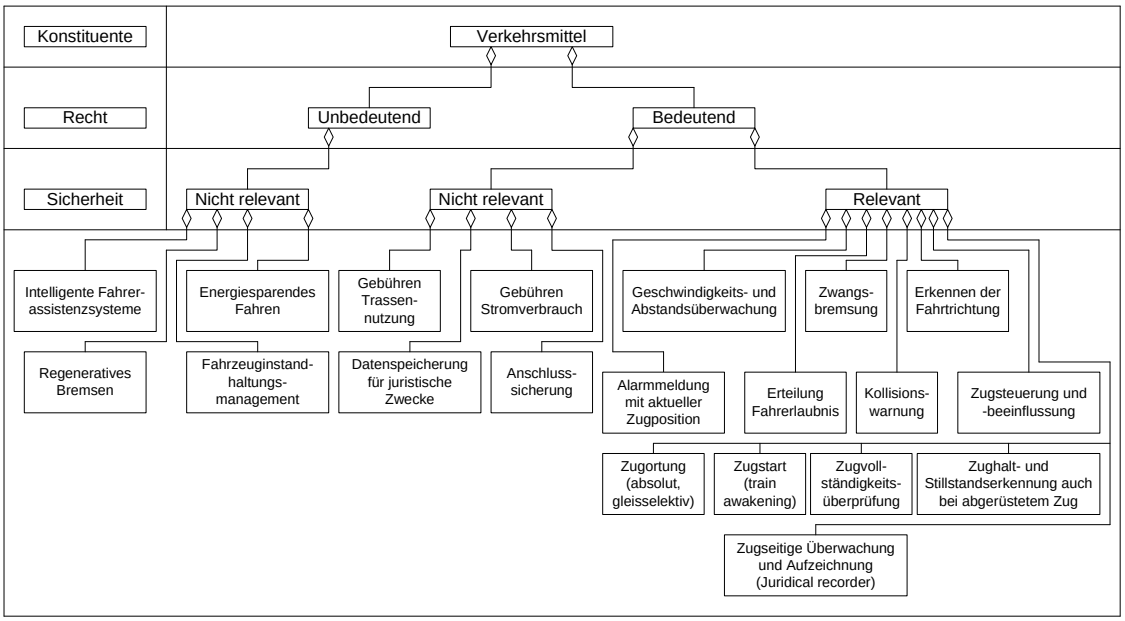


Abbildung 5-4: Anwendungen der Ortung der Kategorie Verkehrsmittel [Meyer zu Hörste 2004; Zukunft et al. 2005; Grimm et al. 2005; Strang 2007; EBA 2012]

Diese Betrachtung wird im weiteren Verlauf dieser Arbeit als Grundlage für die Darstellung der Anforderungen von Anwendungen an die Ortung genutzt. Darauf aufbauend werden in Kapitel 6 die Anforderungen an die Systemkomponenten abgeleitet, was die Grundlage für die Systemarchitektur in Kapitel 7 bildet. Vervollständigt wird die Kategorie Verkehrsmittel mit Anwendungen, welche die Abrechnung von Gebühren und die effiziente Nutzung des Fahrzeugs betreffen.

In Abbildung 5-5 werden alle Anwendungen der Ortung, die der Verkehrskonstituente „Verkehrswegeinfrastruktur“ zugeordnet werden, dargestellt. Auch dort liegt der Fokus auf sicherheitsrelevanten und rechtlich bedeutenden Anwendungen, welche die fahrwegseitige Zugsbeeinflussung und die Durchführung von Gleisarbeiten betreffen.

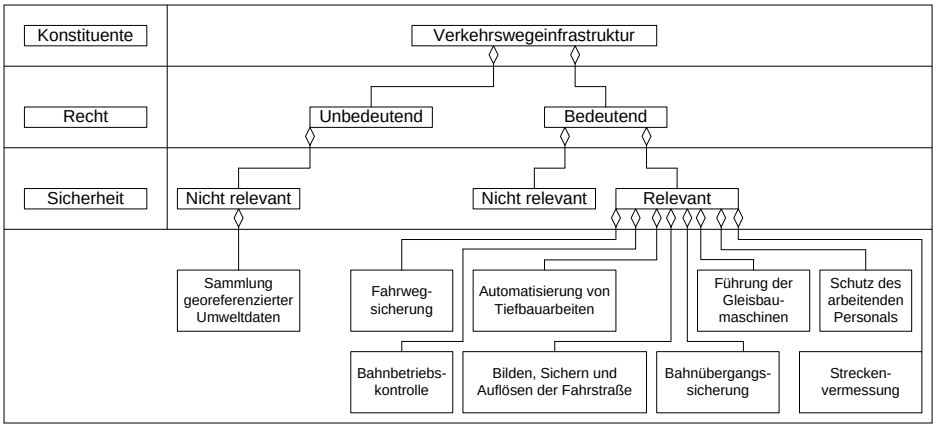


Abbildung 5-5: Anwendungen der Ortung der Kategorie Verkehrswegeinfrastruktur [Meyer zu Hörste 2004; Zukunft et al. 2005; Grimm et al. 2005; Strang 2007]

5.1.3 Zusammenfassung

Im Schienenverkehr existieren hinsichtlich der Verkehrsleittechnik eine Vielzahl an nicht sicherheitsrelevanten, rechtlich unbedeutenden, hinsichtlich des Verkehrsmittels auffallend viele sicherheitsrelevante, rechtlich bedeutende Anwendungen. Diese Tatsache unterstreicht, dass eine Verlagerung der Ortungsverantwortung auf das Verkehrsmittel sinnvoll ist, da dieses die meisten Anwendungen mit den höchsten Anforderungen besitzt, weil dort der Transport stattfindet. Die Verlagerung der Verantwortung von EIU zu EVU sollte sich auch in der Verteilung der Kosten widerspiegeln, bspw. durch eine Reduktion der Trassengebühren. Insgesamt lassen sich aus diesem Vorgehen die Spezifikationen der Ortungseinheit ableiten. Es wird davon ausgegangen, dass sicherheitsrelevante und rechtlich bedeutende Anwendungen die höchsten Anforderungen an die Ortungseinheit stellen, womit die anderen Kategorien ebenfalls berücksichtigt werden. Die relevanten Anwendungen sind, aufgeteilt auf die Verkehrskonstituenten, in Tabelle 5-1 zusammengefasst. Die Strukturierung der Funktionen in anderen Verkehrsdomänen wird in Anhang 4 dargestellt.

Tabelle 5-1: Relevante Anwendungen der satellitenbasierten Ortung im Schienenverkehr

Verkehrsobjekt	Verkehrs-leittechnik	Verkehrsmittel	Verkehrswege-infrastruktur
Bahnsteigbezogene Warnansagen	Fernbedienung von Stellwerken	Alarmmeldung mit aktueller Zugposition	Fahrwegsicherung
Überwachung gefährlicher Güter		Erteilung Fahrerlaubnis	Automatisierung von Tiefbauarbeiten
Warnung der Fahrgäste beim Aussteigen		Kollisionswarnung	Führung der Gleisbaumaschinen
Alarm-, Such- und Rettungsdienst		Zugsteuerung und -beeinflussung	Bahnbetriebskontrolle
		Zugortung (absolut, gleisselektiv)	Bilden, Sichern und Auflösen der Fahrstraße
		Zugstart (train awakening)	Schutz des arbeitenden Personals
		Zugvollständigkeitsprüfung	Bahnübergangssicherung
		Stillstandserkennung auch bei abgerüstetem Zug	
		Zugseitige Überwachung und Aufzeichnung (Juridical recorder)	
		Geschwindigkeits- und Abstandsüberwachung	
		Zwangsbremsung	
		Erkennen der Fahrtrichtung	

5.2 Anforderungen an Stilllegung und Entsorgung

Anforderungen an Stilllegung und Entsorgung sind zwar Teil der normativen Struktur, werden jedoch in dieser Arbeit nicht dargestellt, da sie keinen primären Einfluss auf die sicherheitsrelevante Entwicklung der satellitenbasierten Ortung haben.

5.3 Anforderungen an Betrieb mit externen Einflüssen

Die Anforderungen an den Betrieb mit externen Einflüssen hängen stark vom geplanten Einsatz der Ortungseinheit ab, die hier jedoch nicht bekannt sind. Somit sind lediglich die normativen Mindestanforderungen von Interesse, die bei einem Betrieb der Ortungseinheit auf speziellen Strecken um dort gültige Bedingungen zu ergänzen sind. Als generische externe Einflüsse sind für die Ortungseinheit bspw. Witterungsbedingungen, die geforderte Höhe des Einsatzes über dem Meeresspiegel, der Temperaturbereich sowie EMV zu berücksichtigen. Die dafür relevanten Normen wurden in Abschnitt 3.2.3 dargestellt, ein Überblick über die daraus resultierenden normativen Anforderungen wurde in Abschnitt 3.4.2 und Anhang 5 gegeben.

6 Strukturierung der Sicherheitsanforderungsspezifikationen

In diesem Kapitel werden die aus der Strukturierung in Kapitel 5 resultierenden Anforderungen an die Sicherheit der Ortungseinheit betrachtet, die Anwendung der Ergebnisse erfolgt in Kapitel 7 zur sicheren Systementwicklung.

Die Betrachtung der Sicherheitsanforderungsspezifikationen verfolgt dabei das Ziel, die zu entwickelnde fahrzeugseitige Ortungseinheit als Teil eines Zugbeeinflussungssystems, wie in Abbildung 6-1 dargestellt, nutzen zu können. In dieser Arbeit wird dabei die Ortung fokussiert, Anforderungen an das Stellwerk, Dispositionseinrichtungen wie Betriebsstellen, Betriebsleitstellen, Betriebszentralen und Netzleitzentralen werden nicht dargestellt. Für die Integration in das Zugbeeinflussungssystem sind Schnittstellen zum ERTMS Konzept, insbesondere zu ETCS Level 3, zu erstellen. Die externe Kommunikation ist ebenso nicht Bestandteil dieser Arbeit, es sind lediglich Schnittstellen für die Übermittlung von Fahrtbefehlen (Freie Fahrt, Einschränkung kommend, Halt, etc.) und die Signalisierung zu definieren. Die Signalisierung kann dabei durch Führerstandsignalisierung erfolgen, die mit anderen relevanten Informationen wie Informationen zum nächsten Bahnhof kombiniert werden kann.

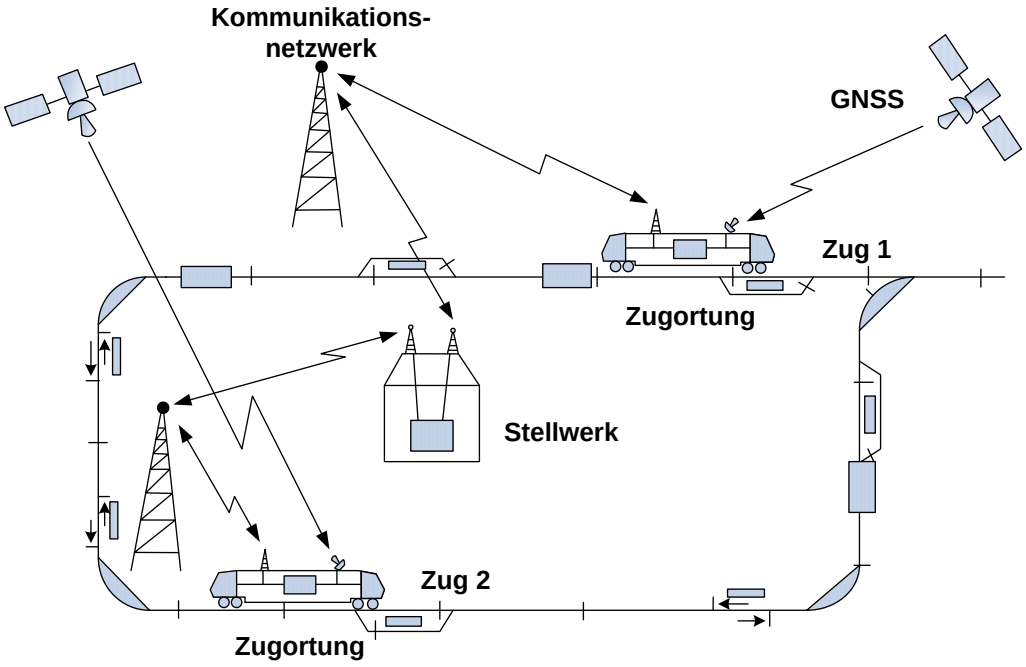


Abbildung 6-1: Zugbeeinflussungssystem mit satellitenbasierter Ortung

In Abschnitt 6.1 werden die Sicherheitsanforderungen aufgestellt, die für einen sicheren Betrieb der Ortungseinheit notwendig sind. Zur Beibehaltung der Kapitelstruktur werden in Abschnitt 6.2 die Anforderungen an die Sicherheitsüberwachung im Betrieb und in Abschnitt 6.3 die Anforderungen an Stilllegung und Entsorgung angeführt. In

Abschnitt 6.4 wird auf die Anforderungen an die Sicherheitserprobung eingegangen, welche vor Inbetriebnahme der Ortungseinheit durchzuführen ist.

6.1 Aufstellen der Sicherheitsanforderungen

In diesem Abschnitt werden die Sicherheitsanforderungen an die zu entwickelnde Ortungseinheit als Grundlage für die anzuwendenden Entwurfsprinzipien, die durchzuführenden Tests und die Sicherheitsanalysen betrachtet. Ortsinformationen sollen kontinuierlich und genau in einem sicherheitsrelevanten Konfidenzintervall geliefert werden. Dafür ist eine stabile Informationsverarbeitung von Bedeutung, die Sicherheit der Ortungseinheit ist von der Qualität der Eingangsinformationen abhängig. Daher ist zu gewährleisten, dass diese unabhängig voneinander generiert werden, da deren Sicherheit sonst nicht getrennt voneinander analysiert werden kann.

Für eine sichere Systementwicklung ist das Aufstellen und Zuordnen der Sicherheitsziele, die von betrieblichen Faktoren wie der geforderten Streckenleistungsfähigkeit und Höchstgeschwindigkeit sowie vom Betriebsverfahren [Klinge 1998] abhängig sind, notwendig. Weiterhin sollte die Ortungseinheit von äußeren Faktoren, wie der Anzahl der sichtbaren Satelliten und deren Signalstärke unabhängig sein. Neben der Sicherheit sind Genauigkeit, Integrität, Verfügbarkeit und Kontinuität der Ortungseinheit zu bewerten [Thomas et al. 2008].

Zu Beginn der Betrachtung der Sicherheitsanforderungen an ein technisches System ist festzulegen, welches Sicherheitsniveau das System erreichen soll. Diese allgemeine Anforderung berücksichtigt nicht die Besonderheiten des jeweiligen Einsatzgebiets. Eine Möglichkeit, die Anforderungen an die Sicherheit spezifisch für die Einsatzbedingungen anzugeben, sind Grenzen oder Konfidenzintervalle, die bspw. bei der Ortung nicht oder nur in begrenzter Anzahl pro Zeiteinheit überschritten werden dürfen. Dieses Vorgehen ist jedoch derzeit im Schienenverkehr nicht als anerkannter Stand der Technik nutzbar und ist daher eine innovative Methode.

In Abschnitt 6.1.1 werden zunächst Anforderungen an die Systemkomponenten dargestellt, in Abschnitt 6.1.2 werden die Anforderungen der Zugbeeinflussung entsprechend den in Abschnitt 4.3.1 durchgeführten Vorarbeiten zum Funktionsaspekt dargestellt. Darauf aufbauend werden in Abschnitt 6.1.3 die Anforderungen an die Ortungseinheit dargestellt, in Abschnitt 6.1.4 die Anforderungen an den Entwicklungsprozess. Anschließend werden in Abschnitt 6.1.5 die Anforderungen an durch Sensoren gelieferte Informationen fokussiert. In Abschnitt 6.1.6 werden technische Sicherheitsanforderungen erörtert.

6.1.1 Anforderungen an Systemkomponenten

Durch das Design der Ortungseinheit sollen gefährliche Fehler der Systemkomponenten und somit des Gesamtsystems ausgeschlossen werden. Für diese Arbeit wird die in [Meyer zu Hörste 2004] durchgeführte Analyse möglicher Gefährdungen und deren Klassifikation genutzt. Es sind Maßnahmen zu treffen, damit die in Abbildung 6-2 dargestellten internen und externen Gefährdungen nicht eintreten.

Abbildung 6-2: Analyse und Klassifikation von internen und externen Gefährdungen [Meyer zu Hörste 2004]

Damit ein Zugbeeinflussungssystem diese generischen und seine weiteren Anforderungen erfüllt, sind Funktionen notwendig. Diese lassen sich nach [Meyer zu Hörste 2004] in strategische, dispositive, taktische und operative Ebenen untergliedern, die Zuordnung der generischen Funktionen zu den Ebenen erfolgt unter Nutzung der Vorarbeiten des iVA [Erdmann et al. 1994; Schnieder 1998; Bikker/Schroeder 2002] und ist in Abbildung 6-3 dargestellt. Aus den dort dargestellten Funktionen eines Zugbeeinflussungssystems lassen sich die Anforderungen an die Ortungseinheit ableiten. Dabei werden lediglich sicherheitsrelevante Funktionen, also die Funktionsgruppen „Steuerung und Sicherung des Fahrwegs“ sowie „Steuerung und Sicherung des Fahrzeugs“ betrachtet. Die strategische, dispositive und taktische Ebene hat geringe Anforderungen an die Ortung und wird daher hier lediglich dargestellt aber nicht zur sicheren Systementwicklung genutzt. Die aus den relevanten Funktionen der operativen Ebene extrahierten Anforderungen werden für die Systemarchitektur in Abschnitt 7.1.2 genutzt. Eine detaillierte Extraktion der Anforderungen erfolgt im folgenden Abschnitt entsprechend des Funktionsaspekts.

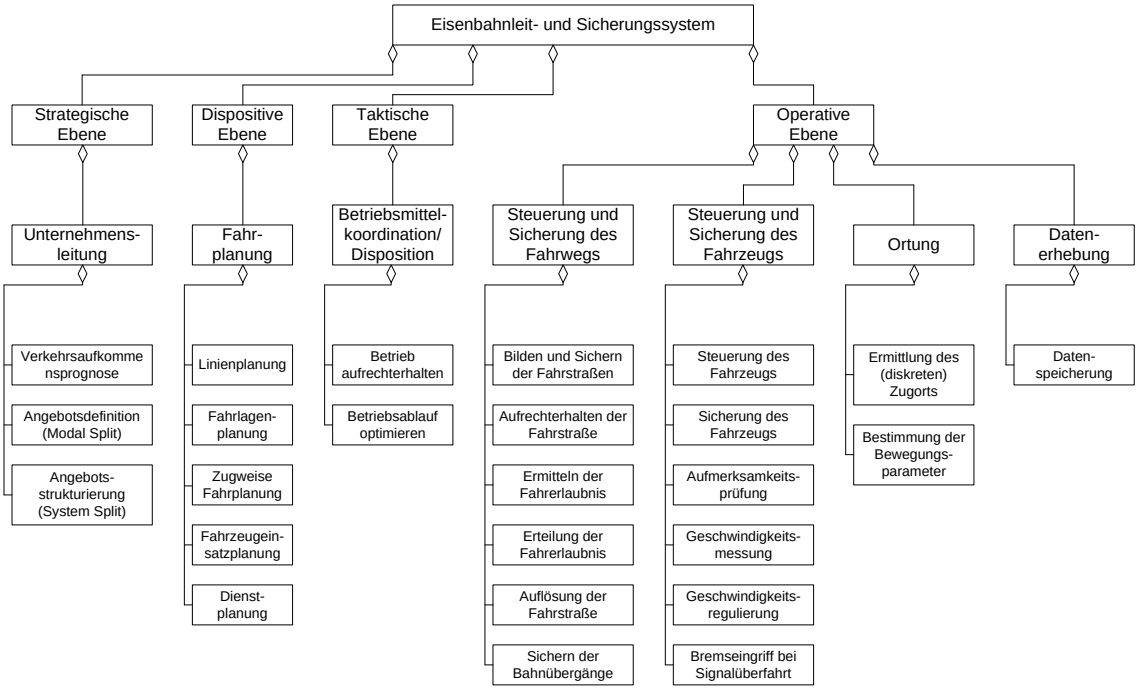


Abbildung 6-3: Generische Funktionen eines Zugbeeinflussungssystems nach [Meyer zu Hörste 2004]

6.1.2 Anforderungen entsprechend des Funktionsaspekts

In diesem Abschnitt wird die in Abschnitt 4.3.1, Abbildung 4-7 eingeführte Gliederung entsprechend des Funktionsaspekts zur Darstellung der Merkmale der Funktionen der satellitenbasierten Ortung genutzt, um gewünschten Funktionen Anforderungen an die satellitenbasierte Ortungseinheit zuzuordnen. Dafür werden zunächst in Abbildung 6-4 alle Funktionen mit dem zur Strukturierung genutzten Funktionsaspekt dargestellt, welche der satellitenbasierten Ortung im Schienenverkehr zugeordnet werden können. Dabei wird deutlich, dass die satellitenbasierte Ortung auch Informationen für nicht sicherheitsrelevante Anwendungen zur Verfügung stellen kann, was einen entscheidenden zusätzlichen Nutzen ohne höheren Aufwand bietet. Ein Beispiel dafür ist die auf die Aufgabe bezogene Funktion „Energie sparendes Fahren“, welche ihre Informationen aus der Funktion „Zugortung im topographischen Profil“ generiert. Der Fahrer durch die Kenntnis vor ihm liegender beweglicher und stationärer Objekte unterstützt werden und die Geschwindigkeit entsprechend regulieren.

Die dargestellte Strukturierung kann auf jede Anwendung der satellitenbasierten Ortung angewandt werden, um deren Funktionsweise und Ziele zu analysieren. Somit können aus Anwendungen im Schienenverkehr, die teils spezifisch (Halt an Bahnsteigkante, Warnen von Gleisarbeitern) und teils generisch (Gleisfreimeldung, Positionsermittlung, Wegstreckenmessung) sind, deren entsprechende Anforderungen extrahiert werden.

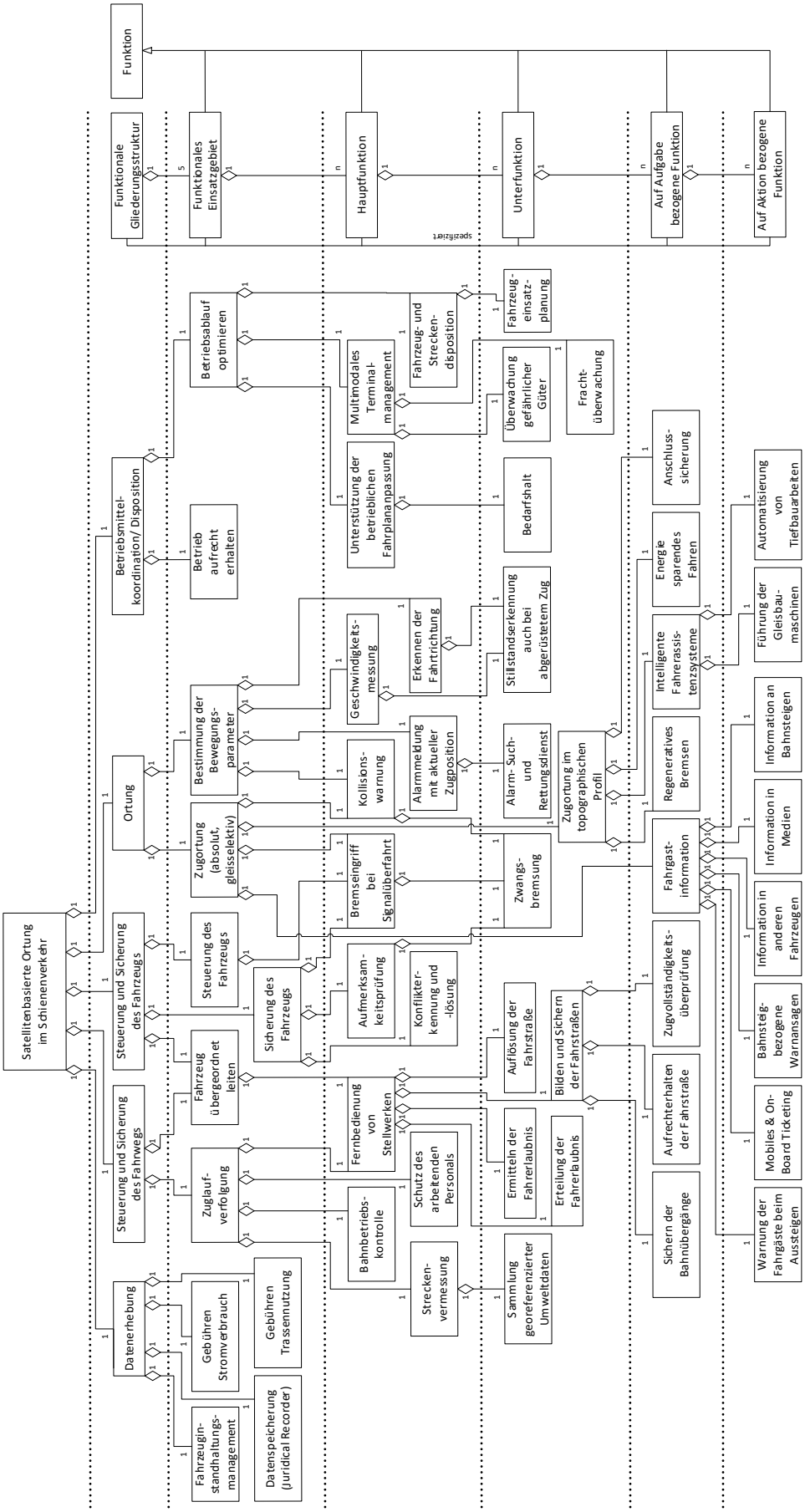


Abbildung 6-4: Funktionsaspekt angewandt auf satellitenbasierte Ortung im Schienenverkehr

6.1.3 Resultierende Anforderungen an die Ortungseinheit

In diesem Abschnitt werden die Anforderungen an die Ortungseinheit mit Bezug auf die geplante Verwendung betrachtet und mit domänenspezifischen Parametern zur Ableitung der Spezifikationen der Bauteile dargestellt. Diese Parameter sind bspw. die Gültigkeit der Informationen, mittlere Lebenszeit (Mean Time Between Failures – MTBF), Fehlzustände und -typen mit ihren Grenzwerten sowie dynamisches Informationsverhalten. Die zulässigen Umgebungsbedingungen und die erlaubten Werte der Prozesszustände sind ebenso zu berücksichtigen.

Aus der Anwendung des Funktionsaspekts in Abbildung 6-4 kann der Betreiber auswählen, welche Funktionen der Ortungseinheit genutzt werden sollen. Deren Anforderungen bilden zusammen mit dem normativen Rahmen die Anforderungen an die Ortungseinheit, die, wie in Abbildung 6-5 dargestellt, in deren Spezifikationen münden. Durch die Kombination der Funktionen soll das Eintreten verschiedener Schadensereignisse, wie bspw. eine Kollision oder eine Entgleisung, vermieden werden. Diese bilden die Grundlage für die in Kapitel 7 entwickelte Ortungsfunktion des Zuges.

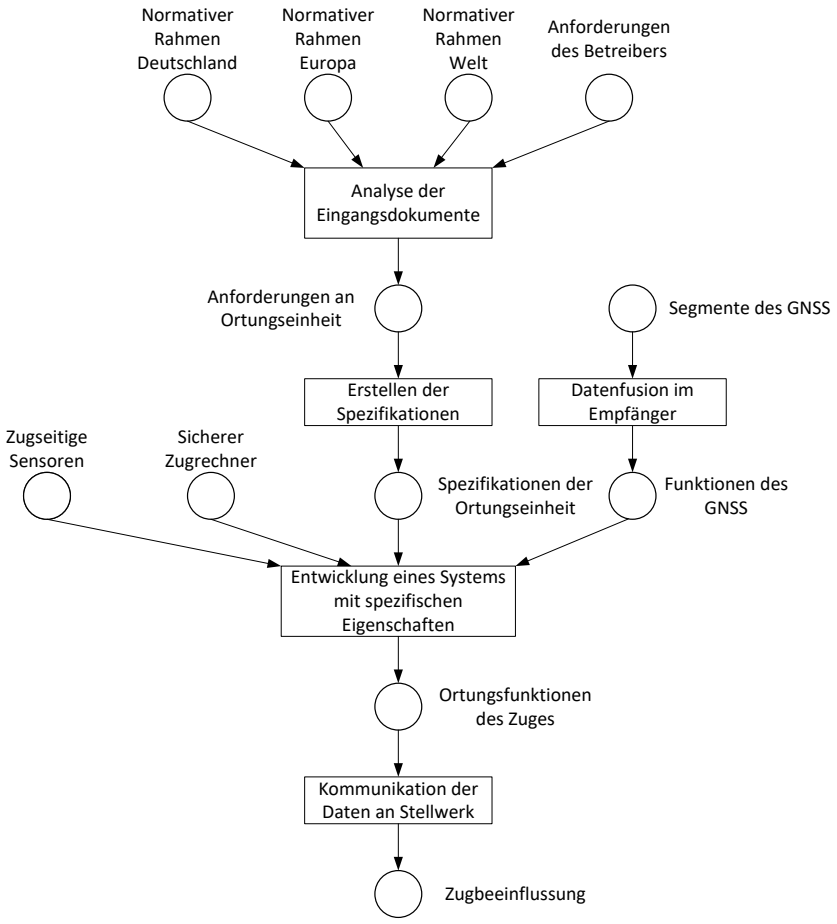


Abbildung 6-5: Anforderungen an Funktion der satellitenbasierten Ortung

Für alle gewünschten Funktionen der Ortungseinheit, die aus den sicherheitsrelevanten Funktionen der Abbildung 5-2 bis Abbildung 5-5 abgeleitet werden, ist durch Anwendung der Attributhierarchie die Darstellung ihrer Anforderungen möglich, was in Abbildung 6-6 beispielhaft für den Bremseingriff bei Signalüberfahrt als Teil der sicheren satellitenbasierten Ortung mit der Methode der Attributhierarchie durchgeführt wird.

Eine Kombination der Anforderungen der gewünschten Funktionen für den Schienenverkehr entsprechend dessen Anforderungen ist exemplarisch in Tabelle 6-1 dargestellt, daraus lassen sich die Spezifikationen der Ortungseinheit ableiten. Die angegebenen Werte können abhängig von der Strecke, auf der die Ortungseinheit eingesetzt werden soll, variieren.

Tabelle 6-1: Anforderungen an die Ortungseinheit im Schienenverkehr

Funktion/ Komponente	Beschreibung	Unterer Grenzwert	Oberer Grenzwert
Tolerable Hazard Rate (THR), SIL-Wert	Zulässige Gefährdungsrate	10^{-9} (SIL 4)	10^{-7} (SIL 2)
Ortungsgenauigkeit bis zu 160 km/h	In Fahrtrichtung	10 m	100 m
	Gleisselektivität	>0 m	2 m
	Senkrecht zur Fahrtrichtung	>0 m	2 m
Sicheres Fehlerverhalten	Sicherheitsrelevante Reaktion	Innerhalb 1 Sekunde	Innerhalb 1 Sekunde
Datenfusion	GNSS-Signale	1 sek	5 sek
	Wirbelstromsensor	1 sek	5 sek
	Digitale Streckenkarte	1 sek	5 sek
Systementwurf	Übertragung der Zugposition	1 sek	5 sek
Software	Sicherheitsrelevant	SIL 3	SIL 4
	Nicht sicherheitsrelevant	SIL 2	SIL 0
Hodometer	Hodometerfehler	-	< 3 σ
GNSS-Empfänger (Zeit bis zur ersten Positionsberechnung)	Fabrikstart	180 sek	-
	Warmstart	90 sek	-
	Kaltstart	180 sek	-
	Heißstart	20 sek	-

Aus den Anforderungen an die Ortungseinheit lassen sich die Anforderungen an die Komponenten, bspw. an den GNSS-Empfänger, ableiten. Für diesen werden in [Lu 2014] 10 m Genauigkeit, eine Zuverlässigkeit von $\lambda < 2*10^{-4}$/h, eine Verfügbarkeit von 99,98 % und eine zulässige Gefährdungsrate von $\lambda \leq 4{,}77*10^{-6}$/h angegeben.

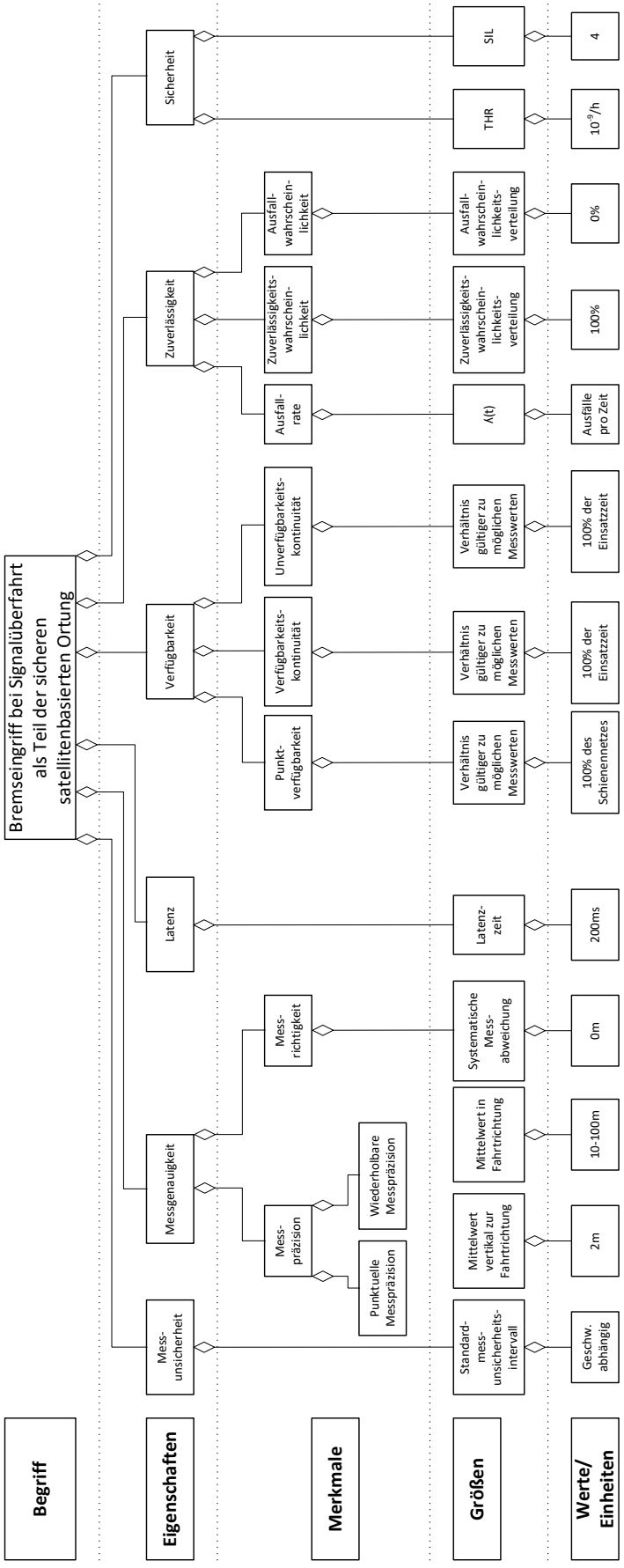


Abbildung 6-6: Anforderungen einer beispielhaften Anwendung an die Ortung/ Funktion

6.1.4 Anforderungen an den Entwicklungsprozess

Im Zuge des Entwicklungsprozesses für eine Zertifizierung einer satellitenbasierten Ortungseinheit mit Nutzung von nicht im Schienenverkehr entwickelten industriellen Komponenten muss dem normativen Rahmen unter Berücksichtigung spezieller Anforderungen des Anwendungsfalls entsprochen werden. Daher sollte die Entwicklung generisch mit der Möglichkeit, Komponenten modular auszutauschen oder hinzuzufügen, erstellt werden. Damit wird die Anpassbarkeit der Entwicklung anderer externer Industriekomponenten zur sicherheitsrelevanten Nutzung, genau wie die Einsetzbarkeit auf verschiedenen Streckenkategorien oder für verschiedene Anwendungen, ermöglicht.

Auf Strecken einer Kategorie mit geringeren Anforderungen an die Ortung kann unter Umständen eine weniger umfangreiche Ortungseinheit eingesetzt werden. Dabei ist jedoch zu beachten, dass diese nicht mehr für Anwendungen mit höheren Anforderungen eingesetzt werden kann und darf.

6.1.5 Anforderungen an durch Sensoren gelieferte Informationen

Die Sensoren müssen durch ihre Funktion und ihr Design dazu beitragen, dass die in Abbildung 6-2 dargestellten internen und externen Gefährdungen nicht eintreten und die entsprechend des in Abbildung 6-6 beispielhaft angewandten Konzepts erarbeiteten Anforderungen erfüllt werden. Damit die Position des Zuges zu jedem Zeitpunkt der Fahrt bekannt ist, ist die Echtzeitfähigkeit der Ortungsinformation zu gewährleisten. Zudem altern von den Sensoren gelieferte Informationen, weswegen diese mit einem Zeitstempel zu versehen und möglichst unverzüglich zu verarbeiten sind. Dafür ist es notwendig, dass die Systemzeiten aller verwendeten Rechner miteinander synchronisiert sind. Unabhängig davon sind die Informationen einer Konsistenz- und Gültigkeitsüberprüfung zu unterziehen und ab einem bestimmten Alter, also wenn ihre Sensierung bereits eine bestimmte Zeitdauer zurückliegt, zu verwerfen. Die Anzahl der verworfenen Informationen in einem Zeitraum sollte jedoch begrenzt sein, bspw. auf eine von zehn Informationen. Wenn festgestellt wird, dass eine Informationsquelle fehlerhaft ist oder den Gültigkeitsbereich verlässt, muss diese innerhalb einer Ausfalloffenbarungszeit isoliert werden. Mit diesem Vorgehen wird die Aktualität der Ausgabewerte des signaltechnisch sicheren Rechnersystems nachprüfbar sichergestellt.

6.1.6 Technische Sicherheitsanforderungen

Die Sicherheit und Verfügbarkeit der Ortungseinheit zur Nutzung für Zugbeeinflussungssysteme ist ohne andere Systeme als Rückfallebene sicherzustellen.

Zudem sind über die Schnittstellen Vorkehrungen zu treffen, die Kommunikation vom Zug zum Stellwerk zu ermöglichen. Dabei sollten Latenzinformationen der Netze berücksichtigt werden, da diese unter Umständen nicht immer zur Verfügung stehen.

6.2 Anforderungen an Sicherheitsüberwachung im Betrieb

Die Anforderungen an die Sicherheitsüberwachung im Betrieb beziehen sich auf die einzuhaltenden Bedingungen, um den Betrieb sicher durchführen zu können. Dabei sollte sichergestellt werden, dass alle Funktionen entsprechend den gestellten Anforderungen durchgeführt werden und keine Gefährdungen nach außen verursachen und nicht von äußeren Einflüssen negativ beeinflusst werden können.

Neben der sicheren Entwicklung des Systems ist die Überwachung der sicheren Durchführung des Betriebs von wesentlicher Bedeutung, womit eine stetige Verbesserung der Betriebsdurchführung erreicht wird.

6.3 Anforderungen an Stilllegung und Entsorgung

Von einem technischen System darf auch nach Ende seiner technischen Lebenszeit keine Gefährdung ausgehen, dieser Aspekt muss bereits bei der Konzeption des Systems berücksichtigt werden. Die Stilllegung und Entsorgung ist daher bei der Systemkonzeption zu berücksichtigen.

6.4 Anforderungen an Sicherheitserprobung

Die Sicherheitserprobung ist ein wesentlicher Bestandteil des Entwicklungsprozesses. Dabei wird untersucht, ob ein technisches System unter den gewünschten betrieblichen Bedingungen entsprechend der Anforderungen an Betrieb und Sicherheit funktioniert. Sie ist bereits während der Entwicklung an einzelnen Komponenten zu beginnen und nach Fertigstellung über einen möglichst langen Zeitraum fortzusetzen.

Damit wird aufbauend auf dem theoretischen Nachweis der Genauigkeit und der Ausfallsicherheit der Komponenten der praktische Nachweis durch Tests als essentieller und wesentlicher Bestandteil eines sicherheitsgerichteten Entwicklungsprozesses durchgeführt. Die notwendigen Tests sollten vor der Migration unter verschiedenen betrieblichen Bedingungen mit verschiedenen Sichtverhältnissen zu den Satelliten ohne Beeinträchtigung des Betriebsablaufs durchgeführt werden [Thomas et al. 2008].

Die Sicherheitserprobung speziell für sicherheitsrelevante Anwendungen ist vor Beginn des Regelbetriebs eines technischen Systems durchzuführen und zu protokollieren. Dieser Test der Leistungsfähigkeit des Ortungssystems kann mit Simulationen oder einem Referenzmesssystem unterstützt werden [Marais et al. 2008]. Dabei sind allgemeine Sicherheitsanforderungen zu beachten, so soll bspw. die in Tests gefahrene Geschwindigkeit 10 % über der Entwurfsgeschwindigkeit liegen. Dauer und Ausmaß der durchzuführenden Tests sowie Maßnahmen, welche die Sicherheit des Schienenverkehrs während den Tests gewährleisten, sind mit der zuständigen Sicherheitsbehörde abzustimmen.

Die Tests vor Inbetriebnahme sollten mindestens ein Kalenderjahr andauern, um alle jahreszeitlichen Aspekte abdecken zu können. Zudem erscheint eine Dauer von mindestens zehn Systemjahren sinnvoll, also bspw. der Test von zehn Fahrzeugen über ein Jahr. Über Tests ist es dennoch nicht nachweisbar, ob ein technisches System SIL 4, was einer Gefährdungsrate von 10^{-9} pro Stunde entspricht, erfüllt. Bei angenommenen 18 Betriebsstunden eines Zuges pro Tag und 365 Betriebstagen im Jahr wären durchschnittlich 152.207 Systemjahre bis zum durchschnittlichen Eintritt des ersten Ausfalls notwendig, zudem sind Abweichungen der statistischen Signifikanz zu beachten. Dies zu testen stellt eine unüberwindbare Herausforderung dar, da eine solch lange Testphase nicht realisierbar ist.

Zum Nachweis der sicheren Funktionalität sind Simulationen, Tätigkeiten im Labor, Feldtests und Betriebstests entwicklungsbegleitend durchzuführen. Zunächst werden fertiggestellte Software oder deren Teile implizit getestet. Nach der Fertigstellung von Komponenten oder Teilsystemen können sich Labortests anschließen, welche als implizite Tests bezeichnet werden. Darauf folgen Feldtests und Betriebstests, die als explizite Tests zusammengefasst und am System oder einem entsprechenden Vormodell durchgeführt werden. Feldtests werden nach Implementierung der durch Labortests festgestellten notwendigen Änderungen zum Detektieren verschiedener Fehlerquellen durchgeführt, um eine kontinuierliche Verbesserung des Produkts zu erreichen. Die Feldtests erster Entwicklungsergebnisse sollten in räumlicher Nähe zum Hersteller durchgeführt werden, um auf festgestellte Mängel kurzfristig reagieren zu können. Diese intensiven Tests ermöglichen eine fundierte Beurteilung der betrieblichen, technischen und funktionalen Eigenschaften der Ortungseinheit. Bestandteil der durchzuführenden Begutachtung ist eine Vor-Ort Begutachtung der Tests und eine detaillierte Situationsanalyse. Verschiedene Testszenarien sind nach detaillierter, dokumentierter Planung durchzuführen, die Ergebnisse sind ebenso detailliert und nachvollziehbar darzustellen. Die Testszenarien sollen sicherstellen, dass die implementierten Funktionen entsprechend den Anforderungen zur Verfügung stehen.

Um auch nach der Inbetriebnahme umfassende Informationen über das Betriebsverhalten des Systems zu erhalten, sind Betriebstests, die ebenso explizite Tests sind, vorzusehen. Deren Prüfbedingungen sollten in Bezug zum System stehen, der Umfang sowie technische und betriebliche Bedingungen sind zusammen mit relevanten Statistiken festzulegen. Darauf aufbauend sind die Prüfdurchführung und deren Dokumentation zu konzipieren und der technische und betriebliche Rahmen der Prüfung, also Umgebung und das Zielsystem zu beschreiben.

Die nach Abschluss der Tests durchzuführende statistische Auswertung fließt entsprechend ihrer Relevanz in die weitere Entwicklung und die Nachweisführung ein. Durch eine Validierung wird geprüft, ob das Produkt entsprechend den gestellten Anforderungen für den vorgesehenen Einsatzzweck entwickelt wurde.

Die Ergebnisse der Tests lassen sich auf Fahrzeuge mit dem gleichen Motorisierungstyp, der gleichen Verbindung der Achsen und der gleichen Position der Achsen anwenden. Bei Tests der Hodometrie sind die Antigleit- und Antischleudereigenschaften des Systems von besonderer Bedeutung. Entsprechend der Motorisierung und/ oder Bremse an der Achse ist dort Schlupf/ Rutschen möglich. Die Tests sollten getrennt für Lokomotive, Triebwagen und Steuerwagen durchgeführt werden. Für die entsprechenden Tests bietet sich bspw. der Einsatz von Seifenwasser unter den Rädern an, um so die korrekte Funktionalität zu testen. Dabei wird mit konstanter Geschwindigkeit das Brems- oder Beschleunigungsverhalten bei einem vorgeschriebenen Geschwindigkeitsprofil getestet. Um realistische Bedingungen zu simulieren, werden nacheinander verschiedene Sensoren abgeschaltet und bspw. bei der Durchfahrt durch Tunnel getestet. Die Validierung durch Tests ermöglicht sichere und stimmige Geschwindigkeits- und Distanzmessungen sowie die Überprüfung einer ergonomisch akzeptablen Anzeige.

Nach Erstellung der Anforderungen in den Kapiteln 5 und 6 wird in Kapitel 7 der Sicherheitsnachweis betrachtet.

7 Erstellung des Sicherheitsnachweises

Im Sicherheitsnachweis wird die sichere Systementwicklung formal und projektspezifisch mit dem Ziel der Vollständigkeit dokumentiert, er ist zu versionieren und vor seiner Weitergabe freizugeben. Im Sicherheitsnachweis ist es von Bedeutung, dass alle für das Erreichen des Sicherheitsziels notwendigen spezifischen Techniken und Maßnahmen abgedeckt werden. Falls gewisse Punkte nicht vollständig abgedeckt wurden, können sicherheitsbezogene Anwendungsbedingungen erstellt werden, ohne deren Implementierung die Gesamtsicherheit des Systems gefährdet ist. Dabei werden zum jeweiligen Stand der Entwicklung bestehende Mängel aufgelistet und Vorschläge zu deren Behebung angeboten.

Im Sicherheitsnachweis ist zu belegen, dass die Entwicklung des technischen Systems entsprechend des in Kapitel 3 dargestellten normativen Rahmens durchgeführt wurde. Dabei sind die zugrunde liegenden Dokumente zu referenzieren, womit deren Kenntnis und Verwendung nachgewiesen wird. Die strukturierte Darstellung des Sicherheitsnachweises wird durch Literatur-, Tabellen- und Abbildungsverzeichnisse ergänzt, zudem ist eine Darstellung der Zertifikate, welche die beteiligten Institutionen besitzen, empfehlenswert. Zusätzlich wird im Sicherheitsnachweis auf die entwicklungsbegleitende Dokumentation verwiesen, in der auch zwischenzeitliche Fortschritte und somit die Entstehung des entwickelten Produkts nachzuvollziehen sind. Dabei fließen hier Ergebnisse aus der in Abbildung 3-8 erstellten Struktur des Sicherheitsnachweises ein.

In diesem Kapitel werden die für die Erstellung eines Sicherheitsnachweises notwendigen Schritte als Teil der sicherheitsgerichteten Systementwicklung betrachtet. Die in den Kapiteln 5 und 6 erarbeiteten Anforderungen an die geplante Anwendung werden zur Entwicklung des umfassenden Nachweises der Systemsicherheit genutzt und fließen in die Dokumentation des Sicherheitsnachweises in diesem Kapitel ein. Die Ergebnisse werden im Sicherheitsgutachten in Kapitel 8 dargestellt.

Der Sicherheitsnachweis beginnt mit der Systemarchitektur und Aspekten der sicheren Systementwicklung in Abschnitt 7.1. In Abschnitt 7.2 folgen allgemeine Informationen, hauptsächlich bezüglich des Qualitäts- und Sicherheitsmanagements. In Abschnitt 7.3 wird die umfangreiche technische Sicherheitsanalyse betrachtet, worauf der Abschluss des Sicherheitsnachweises mit einer Zusammenfassung und Schlussfolgerung in Abschnitt 7.4 folgt. Aufgrund der Bedeutung ist die Struktur dieses Kapitels in Abbildung 7-1 zusammengefasst.

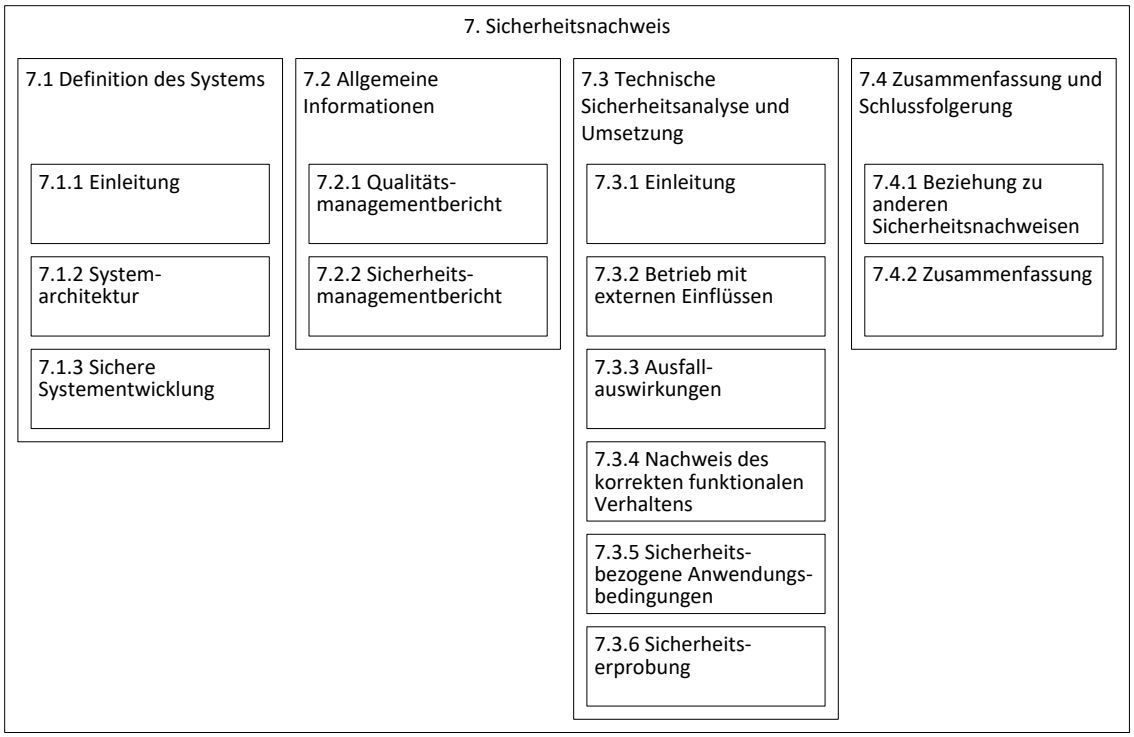


Abbildung 7-1: Struktur dieses Kapitels und des betrachteten Sicherheitsnachweises

7.1 Definition des Systems

In diesem Abschnitt erfolgt die Definition des Systems unter Nutzung der in Kapitel 3 eingeführten Struktur zur Beschreibung eines technischen Systems. Nach einer Einleitung in Abschnitt 7.1.1 wird in Abschnitt 7.1.2 die Systemarchitektur der Ortungseinheit beschrieben. Darauf aufbauend werden in Abschnitt 7.1.3 Aspekte der sicheren Systementwicklung unter Nutzung des Modells der Risikogenese betrachtet.

In der Definition des Systems werden alle wesentlichen Bestandteile erläutert. Für das Verständnis des entwickelten Systems bieten sich eine Referenzierung und Erläuterung der Ausschreibungsunterlagen und Vertragsdokumente an.

Um die satellitenbasierte Ortungseinheit entsprechend der gestellten Anforderungen zu entwickeln, sind auf deren Basis die zu erfüllenden Funktionen zu erstellen, die wiederum die Grundlage für die Spezifikationen des Systems bilden. Dafür wird die in Abschnitt 4.3 eingeführte Methodik der Systemstrukturierung angewandt. Entsprechend wird analysiert, welche Eigenschaften, Merkmale und Größen die Funktionen haben sollen, die durch die satellitenbasierte Ortung gewährleistet werden müssen, um für die Zugbeeinflussung nutzbar zu sein. Daraus lassen sich im Entwicklungsprozess nachweisbare Grenzwerte für die Ortungseinheit und deren Betrieb ableiten.

Bereits bei der Erstellung der Systemarchitektur fließen Gedanken zur Migration ein, deren Stand der Technik in Kapitel 2.2 eingeführt wurde. Dafür wird im Folgenden der in [Obrenovic 2009] vorgeschlagene Migrationsprozess genutzt, um eine Grundlage für die Migration von einem traditionellen Zugbeeinflussungssystem zu einem satellitenbasierten, mit ETCS kompatiblen System zu legen. Nach [Obrenovic 2009] beginnt die Migration mit einer Sicherheitsanalyse und einer Analyse der Ausgangssituation, in denen bspw. der erwartete Empfang der Satellitensignale und Kommunikationsverbindungen untersucht werden. Auch ist das zu nutzende Stellwerk, dessen notwendige Umrüstung oder Neuinstallation und die technischen Möglichkeiten der Installation der Ortungseinheit zu untersuchen und zu entscheiden, ob die Fahrzeuge liniengebunden oder flexibel im Betriebsnetz eingesetzt werden sollen.

In der folgenden Systemselektion sind die technischen Komponenten anhand der notwendigen zur Verfügung zu stellenden Informationen auszuwählen, weiterhin sind die Kommunikation und der Empfang der Satellitensignale sicherzustellen. Die anschließende Entwicklung der Migrationsstrategie beinhaltet die Erstellung des digitalen Kartenmaterials mit zugehörigen Datenbanken und Rechnersystemen, Kommunikation und Ortung. Vor Einführung der Migration sind die Strategien zu bewerten und eine Lösung zu finden. Da keine streckenseitige Infrastruktur existiert, ist eine Einführung unabhängig vom bestehenden Zugbeeinflussungssystem möglich.

7.1.1 Einleitung

Die aus den Anforderungen hergeleiteten Spezifikationen sind Grundlage für die Entwicklung und die Implementierung, die aus einer begründet gewählten Programmiersprache zusammen mit einem geeigneten Betriebssystem, einer Softwarearchitektur, notwendigen Tests und der zugehörigen Dokumentation besteht. Zusätzlich sind Hard- und Softwareschnittstellen zu definieren und zu realisieren.

Die Definition des Systems dient als Grundlage für die Beschreibung der Betriebsprozesse und deren kausaler Folgen. Dabei sind Zweckbestimmung, die gewünschten Funktionen, die Systemgrenzen, physische und funktionale Schnittstellen, die Systemumgebung und bestehende Sicherheitsmaßnahmen von Bedeutung [Schweinsberg 2011]. Durch die zugehörige Modellierung kann das betriebliche Risiko evaluiert werden und somit neben der beabsichtigten Nutzung auch der vorhersehbare Missbrauch betrachtet werden [Schnieder et al. 2009b], wofür die in Abschnitt 4.2.1 eingeführten CSM genutzt werden können. Basierend auf der möglichen Nutzung des Systems ist die Gefährdungsanalyse durchzuführen, womit mögliche Schadensursachen identifiziert und aufgelistet werden können [Schnieder et al. 2009b]. Dabei sind alle

Phasen des Lebenszyklus von Montage über Betrieb und Instandhaltung bis zur Entsorgung und Verwertung einzubeziehen. Darauf aufbauend findet eine Risikoabschätzung und -bewertung statt. Bereits in der Entwurfsphase sollten Maßnahmen zur Risikoreduzierung durchgeführt werden und die Grundlage für die Risikoreduzierung in der Betriebsphase gelegt werden [Schnieder et al. 2009b].

7.1.2 Systemarchitektur

Die Darstellung der Systemarchitektur sollte aus Gründen der Verständlichkeit graphisch erfolgen [Maguire 2006]. Damit können Systemgrenzen eindeutig dargestellt werden, was für die strukturierte Durchführung einer sicheren Systementwicklung von großer Bedeutung ist. Dieses Vorgehen ermöglicht es dem Sicherheitsingenieur, Probleme und Schwierigkeiten zu erkennen und adäquate Lösungen zu erarbeiten, um diese frühzeitig in die Systementwicklung einfließen lassen zu können. Die Systemarchitektur wird so ausführlich wie nötig dargestellt, da ein zu gering strukturiertes System im Verlauf der Entwicklung und Zertifizierung zu erheblichem Mehraufwand führen kann [Braband 2005]. Um diese Darstellung trotzdem verständlich zu halten, wird sie so kurz wie möglich erstellt.

Die Verbindung der Systemarchitektur mit dem Modell des Verkehrsprozesses und dessen Funktionen ermöglicht die Ermittlung der Sicherheitsziele für jede Systemkomponente in Form von tolerierbaren Ausfallraten [Slovak 2006]. Wenn nachgewiesen werden kann, dass durch die genutzte Systemarchitektur die funktionalen Sicherheitsziele erreicht werden, kann die technische Implementierung umgesetzt werden. Wird festgestellt, dass die Ziele auf diesem Weg nicht erreichbar sind, sind die technischen Spezifikationen mit weiteren Maßnahmen zur Steigerung der Verlässlichkeit zu erweitern. Diese Maßnahmen können bspw. Überwachung von Komponenten oder deren redundante Verwendung sein. Zusammenfassend lässt sich die modellbasierte Sicherheitsanalyse in Anforderungsanalyse (Modellierung des Verkehrsprozesses), funktionales Design (funktionale Synthese und globale Modellierung der Verlässlichkeit) und technisches Design (technische Synthese und lokale Modellierung der Verlässlichkeit) untergliedern [Slovak 2006].

Die Beschreibung der Systemarchitektur basiert auf in [DIN EN 50129] empfohlenen bzw. deutlich empfohlenen Techniken und Maßnahmen. Diese sind die Trennung von sicherheitsrelevanten Systemen von nicht sicherheitsrelevanten Systemen und die Begründung der Architektur durch quantitative Zuverlässigkeitsanalysen der Hardware sowie eine der folgenden Techniken/ Maßnahmen:

- Einkanalige elektron. Struktur mit Selbsttest und Überwachung (nur SIL 1 & 2)
- Zweikanalige elektronische Struktur (nur SIL 1 & 2)
- Zweikanalige elektronische Struktur basierend auf Fail-Safe-Struktur durch Redundanz mit Fail-Safe-Vergleich
- Einkanalige elektronische Struktur basierend auf der Fail-Safe-Struktur durch unverlierbare Eigenschaften
- Einkanalige elektronische Struktur basierend auf der Fail-Safe-Struktur durch sicherheitsgerichtete Ausfallreaktion
- Diversitäre elektronische Struktur mit Fail-Safe-Vergleich

Die Systemarchitektur ist das Ergebnis der entsprechend den Spezifikationen durchgeführten sicheren Systementwicklung unter Berücksichtigung verschiedener Aspekte wie Migration und der späteren Verwendung. In Abschnitt 7.1.2.1 wird die Systemarchitektur beschrieben, in Abschnitt 7.1.2.2 die notwendigen Schnittstellen.

7.1.2.1 Beschreibung der Systemarchitektur

Die Systemarchitektur der fahrzeugseitigen Ortungseinheit orientiert sich an einer Standardarchitektur entsprechend des Stands der Technik, die in Abschnitt 2.3.5 eingeführt wurde und in Abbildung 7-2 dargestellt ist. Sie besteht aus absoluter Positionsbestimmung durch GNSS, relativer Wegmessung durch ein domänenspezifisches Hodometer und einer digitalen Streckenkarte.

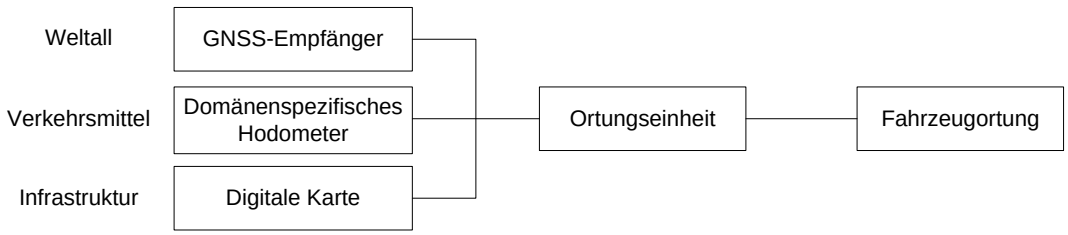


Abbildung 7-2: Standardsystemarchitektur der satellitenbasierten Ortungseinheit

Bei der Spezifikation der Systemkomponenten entsprechend den funktionalen Anforderungen sollten mögliche Störungen, deren Ursachen und die Qualität der Eingangsinformationen in die Betrachtung einfließen. Für die Ortung notwendig sind Informationen über Geschwindigkeit [v], Wegstrecke [s], Richtung und Zeit [t]. Dabei sind die Qualität der Ortung und somit Vollständigkeit, Richtigkeit, Genauigkeit und Konsistenz der Daten von Bedeutung [Plan 2004].

Die Hard und Software des Systems so zu erstellen, dass Ortungsinformationen anforderungsgemäß kontinuierlich zur Verfügung stehen. In der Dokumentation der

entwickelten Software bieten sich Bildschirmfotos an, um Details und deren Implementierung anschaulich darzustellen. Die Dokumentation der Hard- und Softwareentwicklung ist dabei von besonderer Bedeutung, unter anderem weil sie die Grundlage für die nach jedem Entwicklungsschritt durchzuführende Verifizierung und die abschließende, in Kapitel 8 betrachtete Validierung darstellt.

Für eine gleisselektive Ortung im Schienenverkehr sollte die Ortungseinheit aus Sensorik, Ortung und Geodatenbank bestehen [Plan 2004]. Die kontinuierliche Verarbeitung der Sensorausgänge erfolgt in einem echtzeitfähigen System, welches die Ortungsinformationen in festgelegten, kurzen Abständen liefert. Zur Unterstützung der Sensoren können Informationen aus dem Stellwerk bezüglich der Weichenlage und positionsbezogene Informationen über die Abschnittsbelegung genutzt werden.

Der GNSS-Empfänger berechnet seine Position kontinuierlich aus den von den Satelliten gesendeten Positionsdaten und den gemessenen Laufzeiten zwischen Satellit und Empfänger in einem Koordinatensystem, bspw. WGS 84 oder Gauß-Krüger [Septentrio 2011]. Um die Verfügbarkeit des Sensors zu erhöhen, werden alle verfügbaren GNSS, also neben GPS auch GLONASS, Galileo und Beidou genutzt. Durch die Korrekturdaten von EGNOS wird die Genauigkeit verbessert. Dennoch ist aufgrund von Abschattung, Reflexion, Mehrwegausbreitung und Interferenzen bspw. in städtischer Umgebung, in Tunnel, in stark bewaldeten Gebieten oder in Bahnhöfen die GNSS-Ortung nicht ausreichend [Leinhos 1996; Klinge 1998; Teuber et al. 2008]. Daher sind für eine kontinuierliche Ortung, wie bereits in der in Abbildung 7-2 dargestellten Standardarchitektur deutlich wurde, ergänzende fahrzeugseitige Sensoren notwendig. Diese werden im Folgenden auf Basis des in Abschnitt 2.3.4 eingeführten Stands der Technik und der funktionalen Anforderungen ausgewählt.

Nutzbare domänenspezifische Hodometer im Schienenverkehr sind bspw. Radsensoren und optische oder radarbasierte Wegmesser. Inertialsensoren können unterstützend genutzt werden. Die Sensoren sind austauschbar, wenn sie die Anforderungen erfüllen. Verschiedenartige Hodometer haben unterschiedliche Ansprechschwellen, induktive Sensoren liefern bspw. erst ab einer Geschwindigkeit von 0,45 bis 1,34 m/s Messimpulse. Bei Sensoren, welche die Raddrehzahl messen, ist Schlupf sowie die Änderung des Radius des Rades durch Verschleiß, Sinuslauf und Spurspiel zu beachten. Entscheidend sind nicht allein die durch den jeweiligen Sensor genutzten Informationen, sondern darüber hinaus die letztendlich berechnete Position, die auch von weiteren Faktoren wie den Umgebungsbedingungen beeinflusst wird. Um Einflüsse durch Schlupf zu vermeiden, wird sich hier für den Wirbelstromsensor entschieden, da dieser als relativ unempfindlich gegenüber Schlupf gilt.

Eine zu nutzende digitale Karte ist auf dem Auswerterechner installiert und enthält geometrische und topologische Informationen sowie relevante Daten des Verkehrsnetzes [Plan 2004], als Vorbereitung für die Datenfusion sind Filter sinnvoll [Grasso Toro et al. 2012; Grasso Toro 2015]. Die Fusion der Daten des GNSS-Empfängers und des Hodometers erfolgt in der Ortungsfusionskomponente über Koppelortung oder Multisensorverfahren [Geistler 2007; Hasberg 2011].

In der Ortungsfusionskomponente werden die Eingangsinformationen auf Konsistenz geprüft. Das angestrebte Sicherheitslevel des Schienenverkehrs wird durch redundante Strukturen gewährleistet, womit trotz Nutzung industrieller Komponenten die Ortungsinformationen als sicher betrachtet werden können. Zur weiteren Nutzung der Daten wird ein Konfidenzintervall zur betrieblichen Verwendung angegeben.

Die Fusion der Daten der digitalen Karte und der Ortungsfusionskomponente erfolgt in der Ortungseinheit mit Hilfe eines automatischen Kartenabgleichs (Map-Matching) unter Nutzung der Bewegungseigenschaften des Schienenverkehrs. Dabei werden die durch die Ortung ermittelten Daten mit einer digitalen Karte verknüpft [Plan 2004]. Um diesen Vorgang mit der erforderlichen Präzision und Genauigkeit durchführen zu können, sind eine hohe Qualität und Aktualität der digitalen Karte wichtig.

Zur sicheren Ortung des Zuges werden von jedem Sensortyp zwei diversitäre Sensoren verwendet. Durch einen Datenfusionsalgorithmus wird damit die exakte Position des Zuges in Echtzeit berechnet. Zusätzlich hat die Ortungseinheit die Aufgabe, die Gültigkeit der Ortungsinformation durch selbstüberprüfende Algorithmen anzugeben. Aus den anforderungsgemäßen Sensoren lässt sich nach dem Ortsaspekt die Architektur der Ortungseinheit darstellen, wobei auf „Einrichtung/ Gerät“ und „Technische Einrichtung“ verzichtet wird, um den Einbauort darstellen zu können (Abbildung 7-3).

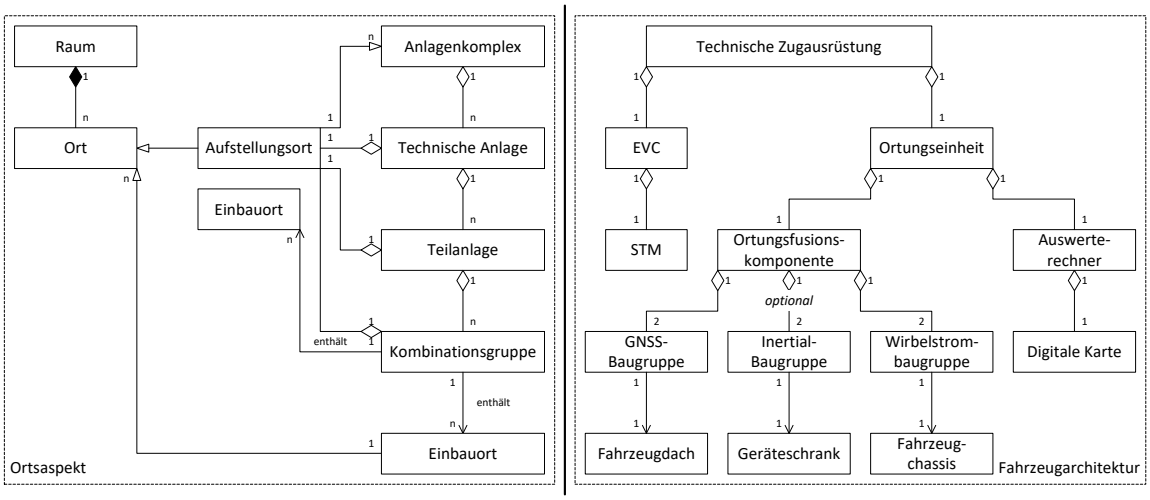


Abbildung 7-3: Fahrzeugarchitektur der satellitenbasierten Ortungseinheit entsprechend des Ortsaspekts

Bei der Fahrzeugarchitektur sind Hard- und Softwareschnittstellen zu berücksichtigen, welche die Übertragung der Informationen von den Sensoren zur Ortungseinheit, von dort zum Zug sowie weiter zum Zugbeeinflussungssystem gewährleisten. Deren Definition wird in Abschnitt 7.1.2.2 näher betrachtet.

7.1.2.2 Definition der Schnittstellen

In diesem Abschnitt werden die Schnittstellen der Ortungseinheit fokussiert. Die Kommunikation zum Bediener wird durch Mensch Maschine Schnittstellen hergestellt, interne Systemschnittstellen verbinden Sensoren mit dem sicheren Rechner. Dies kann mit einem für sicherheitskritische Anwendungen geeigneten Fahrzeugbuskonzept realisiert werden [Bornschlegl 2014]. Externe Systemschnittstellen geben die Ortungsinformation an Anzeigegeräte und das Zugbeeinflussungssystem, welche diese Informationen nutzen sollen, weiter. Eine schnelle Weitergabe der Daten gewährleistet die Echtzeitfähigkeit und somit Kontinuität des Systems.

Zur Visualisierung werden die Schnittstellen zusammen mit der Fahrzeugarchitektur (Abbildung 7-3) der satellitenbasierten Ortungseinheit in Abbildung 7-4 dargestellt. Dabei wird der Ortsaspekt mit dem Funktionsaspekt kombiniert, indem Funktionen verschiedenen Kombinationsbaugruppen zugeordnet werden.

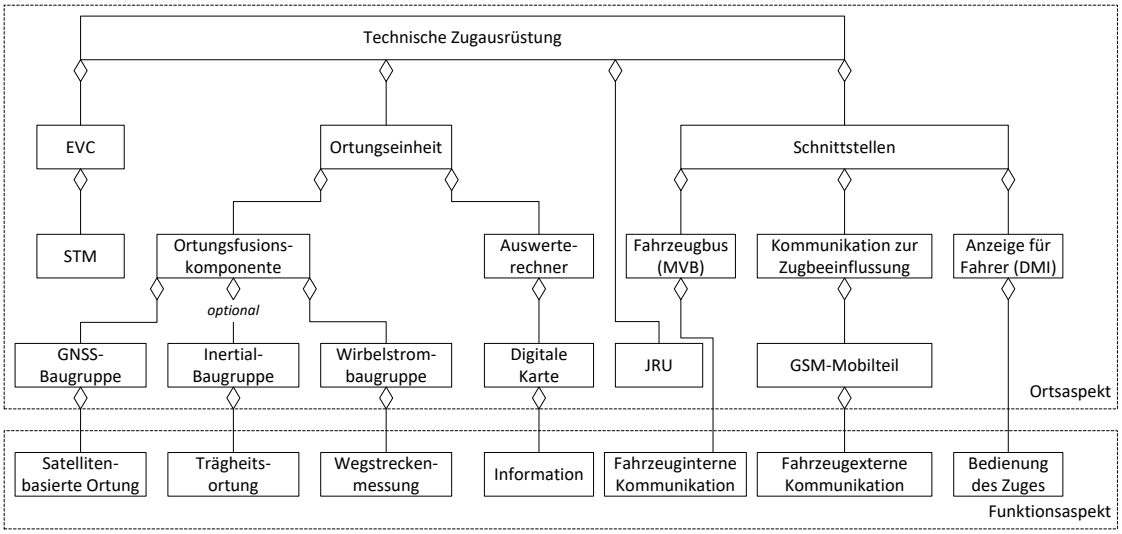


Abbildung 7-4: Fahrzeugarchitektur – strukturierte Sensorankopplung entsprechend des Orts- und Funktionsaspekts

Die Schnittstellen und die Verarbeitung der übermittelten Informationen ermöglichen die Kombination von COTS mit Komponenten, die entsprechend der Eisenbahnzertifizierung entwickelt wurden, zu einer sicheren Ortungseinheit.

Aufgrund der daraus resultierenden Bedeutung der Schnittstellen zu anderen Systemen wird in Abbildung 7-5 die Ortungseinheit zusammen mit in Bezug stehenden Systemen dargestellt, wofür die strukturierte Darstellung des Produktaspekts genutzt wird. Die Ortungseinheit ist schraffiert dargestellt und wird hier als technisches System verstanden, das alle Komponenten umfasst, die für die Ortung genutzt werden.

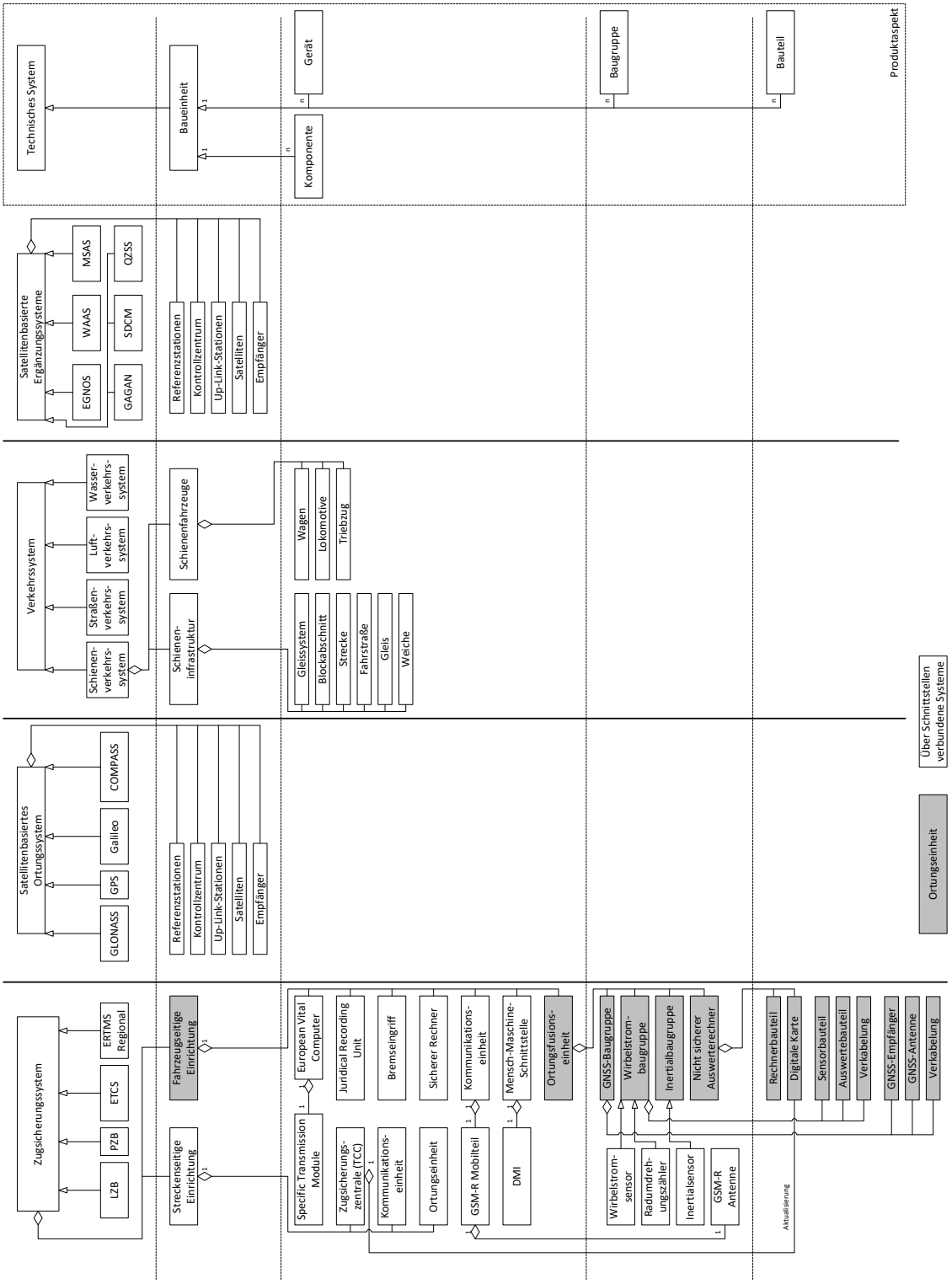


Abbildung 7-5: Fahrzeugarchitektur entsprechend des Produktaspekts

Die strukturierte und vollständige Anwendung der Aspekte ermöglicht es, als Grundlage der Gefährdungsidentifikation alle Systemkomponenten zu offenbaren, an denen potentielle Fehler auftreten können. Damit können alle Gefährdungen dargestellt werden, die einen „unerwünschten Zustand (Schaden) herbeiführen können“ [May 2010]. Mit

diesem Vorgehen können risikoreduzierende Maßnahmen erstellt werden um das Auftreten einer Gefährdung zu verhindern bzw. das Schadensausmaß zu reduzieren.

7.1.3 Sichere Systementwicklung

Die sichere Systementwicklung verfolgt das Ziel, für das in Abschnitt 7.1.2 eingeführte System technische und organisatorische Maßnahmen zu entwerfen, um die Wahrscheinlichkeit eines Komponentenfehlers auf ein Minimum zu reduzieren. Damit wird verhindert, dass während des Verkehrsprozesses Gefährdungssituationen eintreten. Falls dennoch eine Gefährdungssituation eintritt, sollte diese nicht zu einem Unfall oder Schaden führen, wofür eine Gefährdungserkennung notwendig ist, um in den sicheren Verkehrsprozess zurückzukehren [Slovak 2006]. Neben der funktionalen Sicherheit nach [DIN EN 50126; DIN EN 50128; DIN EN 50129] ist die Systemarchitektur von Bedeutung, die funktionalen Sicherheitsziele bilden die Schnittstelle zwischen Risiko- und Gefährdungsanalyse [Slovak 2006]. Die Risikoanalyse ist dabei anhand der Systemdefinition vom Betreiber durchzuführen. Die Sicherheitsanalyse kann mit einer formalen Beschreibung unterstützt werden, womit „die Sicherheitsanforderungen für die Systemfunktionen sowie Systemkomponenten im Sinne der genannten Normen“ [Slovak 2006] definiert und validiert werden können. Dafür ist die Darstellung der Beziehung zwischen dem Auftritt unerwünschter betrieblicher Ereignisse (Schäden) und dem Potenzial des funktionalen Ausfalls einer Komponente (Verlässlichkeit) zu beschreiben. Mit der Maßgabe, dass nur sichere Systemzustände eingenommen werden sollen, findet der Grundgedanke des in Abschnitt 3.3.6 vorgestellten Ansatzes von [Leveson 2011] Anwendung. Zur Umsetzung werden in Abschnitt 7.1.3.1 die genutzten technischen Sicherheitsprinzipien zusammengefasst und in Abschnitt 7.1.3.2 die Projektierung von Teilsystemen sowie der Systemaufbau betrachtet.

7.1.3.1 Zusammenfassung der technischen Sicherheitsprinzipien

In einem technischen System kann ein Diagnosesystem das Messsystem überwachen, deren jeweiligen Zustände sind in Tabelle 7-1 dargestellt. Angewandt auf die satellitenbasierte Ortungseinheit bilden die Sensoren das Messsystem und die Datenfusion zusammen mit dem sicheren Rechner das Diagnosesystem.

Tabelle 7-1: Kombinatorische Verknüpfung der Systemzustände

		Diagnosesystem		
		Betriebsbereiter Zustand	Vorbereitung der Instandhaltung	Korrektive Instandhaltung
Mess-system	Betriebsbereiter Zustand	1	2	3
	Vorbereitung der Instandhaltung	4	5	6
	Korrektive Instandhaltung	7	8	9

Die dargestellten Zustände werden analysiert, um die sicheren Zustände zu extrahieren. Im Zustand 1 ist das System in Betrieb und sicher, bei den Zuständen 4, 5, 6, 7, 8 und 9 nicht im Betrieb und sicher. Bei den Zuständen 2 und 3 ist das Messsystem in Betrieb, jedoch das Diagnosesystem im Zustand der Vorbereitung der Instandhaltung bzw. während der korrektiven Instandhaltung. Diese Zustände sind auszuschließen, da in diesem Fall mögliche Fehler des Messsystems nicht korrekt erkannt werden können. Die Außerinbetriebnahme des Messsystems ist unverzüglich zu veranlassen.

Die sichere Entwicklung eines technischen Systems ist so durchzuführen, dass die Wahrscheinlichkeit des Eintretens einer gefährlichen Kombination, die zu Unfällen führen kann, möglichst gering ist. Sie orientiert sich dabei am sicherheitsgerichteten Entwicklungsprozess im Schienenverkehr und zugehörigen mathematischen Prinzipien, die in Abschnitt 4.1.1 dargestellt wurden. Für eine direkte Anwendung in der Risikobetrachtung eines technischen Systems für GNSS wäre die Zertifizierung der genutzten satellitenbasierten Sensorik hinsichtlich RAMS notwendig [Marais/Beugin 2012]. Da dies jedoch nicht geplant ist, können die Kenngrößen der entwickelten Ortungseinheit nicht mit den in Abschnitt 6.1 dargestellten Sicherheitsanforderungen verglichen werden. Herkömmliche Methoden wie bspw. FMEA oder eine qualitative und quantitative RAMS-Analyse sind somit nicht anwendbar, da die Gefährdungsraten der COTS nicht entsprechend der Normen des Schienenverkehrs anerkannt sind.

Zur Gewährleistung der Sicherheit ohne Nutzung herkömmlicher Methoden sind bereits während der Entwicklung mögliche systematische Fehler, insbesondere bezüglich der Integration von COTS, zu untersuchen und auszuschließen. Für diesen Teil der Risikobetrachtung ist die Struktur des Systems von wesentlicher Bedeutung. Hierbei wird die Annahme getroffen, dass höchstens ein Ausfall zur selben Zeit auftritt. Eine schnelle Detektion der Ausfälle erfolgt z. B. durch eine redundante, zweikanalige diversitäre Struktur und einem mit SIL 4 zertifizierten Rechner kombiniert mit einer schnellen

Fehlerdiagnose. Bei Vergleich mit mehr als zwei Kanälen kann auch ein fehlerhafter Kanalzustand infolge weiterer Informationen erkannt und dieser Kanal ausgeschlossen werden [Schnieder/Schnieder 2013]. Somit sind Maßnahmen wie Redundanz, Diagnostik und Instandhaltungsstrategien zu implementieren, um die technische Sicherheit zu gewährleisten [Schnieder 2009].

Bei der Ausfalldetektion als Teil der Sicherungseinrichtung rückt die Ausführung des Vergleichs bezüglich Funktionalität und Zuverlässigkeit in den Vordergrund. Da der Vergleich sicherheitsrelevant ist, sollte er ebenso mehrkanalig ausgeführt sein [Schnieder/Schnieder 2013]. Mit den dargestellten Maßnahmen ist das technische System in der Lage, trotz eines gefährlichen Zustands die Gefährdung abzuwehren. Ein fehlertolerantes System erfüllt seine Funktion trotz Beeinträchtigung einzelner Komponenten weiterhin und nimmt nach außen einen ungefährlichen Zustand ein.

Um darzustellen, wie das Eintreten eines Schadens verhindert werden kann, wird das Modell der Risikogenese angewandt. Dort wird das Auftreten eines Fehlers als kausale Begründung für ein Risiko beschrieben. Eine potentielle Gefährdung ist dabei ein Zustand, der die Möglichkeit eines Fehlzustands aufweist. Ein Gefährdungsereignis kann einen Schaden hervorrufen, es resultiert der Zustand der Gefährdung als potentielle Schadensquelle. Wenn dieser zeitlich und räumlich mit bestehenden Rechtsgütern (Mensch, Güter, Umwelt) zusammentrifft und sich somit eine Gefährdungssituation ergibt, tritt ein Schadensereignis ein. In Abbildung 7-6 wird dieses Verständnis mit den gewünschten Zuständen kombiniert, um Maßnahmen zur Vermeidung und Abwehr von Gefährdungen abzuleiten.

Der Schaden selbst kann dabei nach seiner Schwere unterteilt werden, bei menschlichen Schäden bspw. in leichte Verletzungen, schwere Verletzungen und tödliche Verletzungen [Schnieder et al. 2009b]. Zur Bewertung des Schadens wird auch die prognostizierte Häufigkeit seines Eintretens betrachtet.

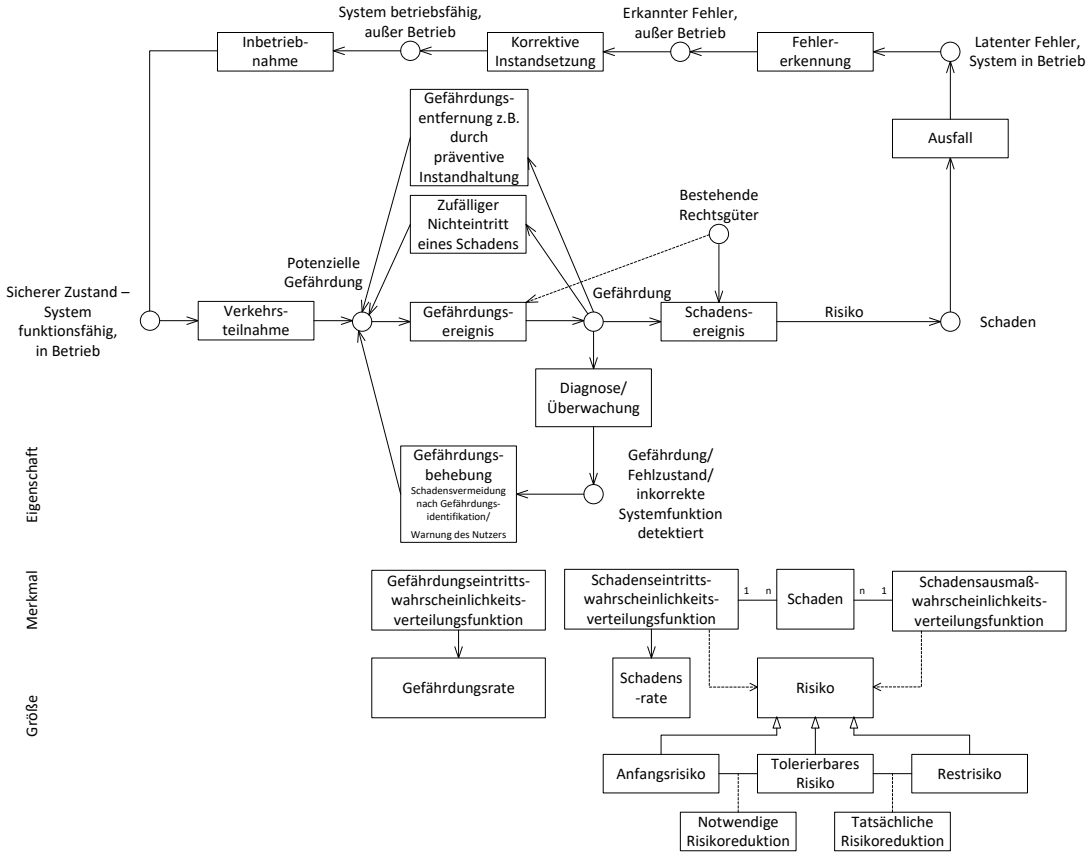


Abbildung 7-6: Modell der Risikogenese kombiniert mit Sicherheitsimplementierung durch Vermeidung und Abwehr von Gefährdungen nach [Drewes 2009; Schnieder et al. 2009b; Schnieder 2010; Schnieder/Schnieder 2013; Müller 2015]

Während der Teilnahme am Verkehr befindet sich ein Verkehrsmittel zusammen mit den transportierten Gütern im Zustand der potentiellen Gefährdung. Daraus können ein Gefährdungsereignis und somit eine Gefährdung resultieren, wenn eine potentielle Ursache für einen Schaden vorliegt. Wenn eine Gefährdung mit einem anderen bestehenden Rechtsgut zusammentrifft kann dies zu einem Schadensereignis des Verkehrsmittels führen. Durch Diagnose, Überwachung, Gefährdungsentfernung (z. B. präventive Instandhaltung) oder zufälligen Nichteintritt des Schadens kann das Verkehrsmittel in den Zustand der potenziellen Gefährdung zurückgeführt werden.

Ziel der sicheren Funktion eines Systems ist, dass möglichst alle Fehler und somit Gefährdungszustände erkannt werden und das System in den sicheren Zustand überführt werden kann. Dafür muss die Diagnose- und Überwachungsfunktion intakt sein. An dieser Stelle wird deutlich, dass die Sicherungsfunktionen bedeutend und sinnvoll sind, da bei Nichterkennen einer fehlerhaften Systemfunktion ein Schaden eintritt. Dabei sollte der Schadenszustand, also die Auswirkung des Schadens, reduziert werden.

Aus dem Modell der Risikogenese und dessen Beschreibung ergeben sich verschiedene Möglichkeiten, den Eintritt des Schadens zu verhindern oder dessen Auswirkungen zu

reduzieren. Dies kann proaktiv durch Ausschluss der potenziellen Gefährdung durch Überführung des Gefährdungsereignisses oder des Gefährdungszustands in einen sicheren Zustand geschehen. Das Zusammentreffen des betrachteten Systems mit einem anderen Rechtsgut, also ein Schadensereignis, wird versucht durch schnelles Erkennen zu verhindern. Bei einem reaktiven oder postaktiven Vorgehen wird versucht, die Folgen des Schadensereignisses zu mindern. Um den Anforderungen gerecht zu werden, müssen die in Abschnitt 6.1.2 erarbeiteten Funktionen sicher in der Ortungseinheit umgesetzt werden.

7.1.3.2 Projektierung von Teilsystemen und Systemaufbau

Die Projektierung von Teilsystemen und der Systemaufbau können mit einem Vergleich zum Altsystem mit dem Nachweis der mindestens gleichen Sicherheit nach den anerkannten Regeln der Technik stattfinden. Aufgrund verschiedener Rahmenbedingungen wie dem nicht bekannten Sicherheitslevel alter Systeme, kann dies unter Umständen nicht realisierbar sein, weswegen dann ein vergleichbarer Nachweis erbracht werden muss. Dieser Vorgang wird als sicherheitliches Ermessen bezeichnet [VV NTZ ÜGR Stufe 2 2013].

Um sicherheitliches Ermessen mit in die Begutachtung einfließen lassen zu können, ist ein Projektteam zu bilden, ein Systemgutachter zu beauftragen, ein Prüfplan zu erstellen und die geplante Zertifizierung dem EBA anzuzeigen [VV NTZ ÜGR Stufe 1 2013]. Als Systemgutachter wird dabei ein „vom EBA anerkannter Sachverständiger mit mehrjähriger Berufserfahrung im Bereich eines Eisenbahnbetriebsleiters einer Eisenbahn des Bundes in betriebssicherheitlichen Ermessensentscheidungen“ [VV NTZ ÜGR Stufe 2 2013] mit dem Schwerpunkt Leit- und Sicherungstechnik bezeichnet. Aufbauend auf einer möglichst breiten Wissensbasis erarbeitet das Projektteam Lösungen, wie die Sicherheit gewährleistet werden kann [VV NTZ ÜGR Stufe 1 2013]. Dabei wird der Prüfplan vom Hersteller gemeinsam mit den Mitgliedern des Projektteams und dem Systemgutachter abgestimmt und dem EBA vorgelegt. Die erforderlichen Nachweise werden vom Hersteller erstellt und vom Gutachter sowie Systemgutachter mit den zugeordneten Schwerpunkten geprüft. Diese werden vom Gutachter mit Fokus auf die Vollständigkeit aller zusammenhängenden Punkte geprüft. Der Systemgutachter und das EBA prüfen die erarbeiteten Lösungen auf korrekte Ausführung in Bezug auf das sicherheitliche Ermessen. Dabei unterstützt der Freigabeverantwortliche eine qualitativ hochwertige Dokumentation und zeigt den Abschluss der Entwicklung unverzüglich beim EBA an. Vorzulegende Dokumente sind der Prüfplan, die Bewertungsergebnisse im Erläuterungsbericht sowie die Prüferklärung. Das EBA ist über eine Betriebserprobung zu informieren, um die Teilnahme zu ermöglichen.

7.2 Allgemeine Informationen

Im Abschnitt „Allgemeine Informationen“ sind Grundlagen der Entwicklung aufzuführen, die allgemein bei den beteiligten Institutionen wie Hersteller und Betreiber gelten, bspw. qualitäts- und sicherheitsbezogene Zertifikate. In Abschnitt 7.2.1 wird auf den Qualitäts-, in Abschnitt 7.2.2 auf den Sicherheitsmanagementbericht eingegangen.

7.2.1 Qualitätsmanagementbericht

Das QMS des Herstellers [DIN EN ISO 9001] sollte auf dessen Anforderungen abgestimmt sein. Dies beinhaltet eine entsprechende Anpassung an sich verändernde Rahmenbedingungen. Zudem ist in der Dokumentation jeweils die Gültigkeit der zur Verfügung gestellten und genutzten Information anzugeben. Es bietet sich bei diesem Vorgehen an, möglichst auf bereits begutachtete Prozesse und Dokumente zurückzugreifen.

7.2.2 Sicherheitsmanagementbericht

Das Sicherheitsmanagement des Herstellers wird genau wie das Qualitätsmanagement in internen Unternehmensprozessen erstellt [DIN EN ISO 9000] und baut auf den normativen Grundlagen [DIN EN 50126], [DIN EN 50128] und [DIN EN 50129] auf. Für die sichere Entwicklung ist die Qualifikation des beteiligten Personals notwendig, was zu dokumentieren ist. Zusätzlich sind Referenzen innerhalb des Dokuments sowie zu anderen Dokumenten von großer Bedeutung, um die Informationen strukturiert darstellen und die Bezüge sowie Dokumente verwalten zu können.

7.3 Technische Sicherheitsanalyse und Umsetzung

Der Abschnitt „Technische Sicherheitsanalyse und Umsetzung“ ist der wesentliche Bestandteil der Sicherheitsnachweisführung, die in Abschnitt 3.3 eingeführt wurde. Er besteht insbesondere aus dem technischen Sicherheitsbericht. Darin erfolgt der Nachweis der sicheren Systementwicklung, im Fall dieser Arbeit mit einem innovativen Charakter aufgrund der genutzten industriellen Komponenten. Dabei werden unter anderem Ausfallauswirkungen, der Schutz gegen systematische Fehler und die Fehlerbeherrschung betrachtet.

Nach der Einleitung in Abschnitt 7.3.1 wird in Abschnitt 7.3.2 der Betrieb mit externen Einflüssen betrachtet. In Abschnitt 7.3.3 werden Ausfälle, deren Auswirkungen, Offenbarung und notwendige Maßnahmen beschrieben. In Abschnitt 7.3.4 wird der

Nachweis des korrekten funktionalen Verhaltens betrachtet. Darauf folgen in Abschnitt 7.3.5 sicherheitsbezogene Anwendungsbedingungen und in Abschnitt 7.3.6 Aspekte der Sicherheitserprobung.

7.3.1 Einleitung

In der technischen Sicherheitsanalyse und Umsetzung werden die für eine sichere Systementwicklung notwendigen Schritte dargestellt. Die Sicherheit eines technischen Systems kann prinzipiell durch organisatorische Qualifikation, technische Qualifikation und Funktionskonformität erreicht werden [Schnieder 2009]. Die organisatorische Qualifikation betrachtet die notwendige Haftung beim Betrieb. Die technische Qualifikation erfolgt durch den Nachweis domänenspezifischer Eigenschaften – hier also für die Domäne Schienenverkehr. Die funktionale Konformität bezieht sich auf die Eingliederung der Funktionen in ein Zugbeeinflussungssystem [Eisweiler/Steinebach 2014].

Durch das in diesem Abschnitt erarbeitete Vorgehen werden technische, wirtschaftliche und soziale Herausforderungen erstmalig gelöst, indem Ideen oder Prozesse, die über den Stand der Technik hinausgehen, sowie deren wirtschaftliche Umsetzung entwickelt werden. Innovationen können dabei in Basisinnovationen, Verbesserungsinnovationen, Anpassungsinnovationen und Scheininnovationen gegliedert werden [May 2010]. Die Durchführung von Innovationen ist mit klaren Zielen verbunden, bspw. die Verbesserung der Qualität des Gesamtsystems entsprechend den Erfordernissen des Betreibers.

Die Herausforderung bei der technischen Sicherheitsanalyse besteht darin, die Entwicklung eines innovativen Systems bei Nutzung des traditionellen Entwicklungsansatzes durchzuführen. Bei einer traditionellen Entwicklung im Schienenverkehr werden die Komponenten und das zu entwickelnde System entsprechend den aufgestellten Anforderungen entwickelt. Bei der hier durchgeführten Integration von der satellitenbasierten Ortung als COTS werden zwar auch Anforderungen aufgestellt, jedoch werden aufgrund dieser keine Produkte entwickelt sondern lediglich Komponenten ausgewählt. Somit kann die sichere satellitenbasierte Ortung in den Schienenverkehr eingeführt werden, was nach dem aktuellen Stand der Technik nicht möglich wäre. Diese Innovation kann als Basisinnovationen betrachtet werden, da Schlüsseltechnologien und neue Organisationsprinzipien verwendet werden, die zur Entwicklung neuer Wirkprinzipien, Produkte und Verfahren führen. Der Nachweis des korrekten funktionalen Verhaltens erfolgt in Abschnitt 7.3.4. Darauf aufbauend kann das Sicherheitsgutachten als nächster bedeutender Schritt in Kapitel 8 erstellt werden.

7.3.2 Betrieb mit externen Einflüssen

In diesem Abschnitt werden externe Einflüsse aufgezählt, unter denen der Betrieb eines technischen Systems im Schienenverkehr möglich sein muss. Die dafür grundlegenden Normen wurden in Abschnitt 3.4.2 und Anhang 3 dargestellt. Externe Einflüsse sind für die System- und Komponentensicherheit von Bedeutung. Die Sicherheit der anderen auf dem Zug installierten Komponenten darf nicht beeinflusst werden, genau wie die anderen Komponenten die Sicherheit der Ortungseinheit nicht beeinflussen dürfen.

Zunächst werden in Abschnitt 7.3.2.1 die klimatischen Bedingungen betrachtet, unter denen ein Betrieb des für den Schienenverkehr entwickelten Systems sichergestellt werden muss. In Abschnitt 7.3.2.2 werden ergänzend die mechanischen Bedingungen geprüft. Ein weiterer Bestandteil der Systematik ist die Höhe über dem Meeresspiegel, bei der dessen Einsatz gewährleistet werden muss, was in Abschnitt 7.3.2.3 fokussiert wird. In Abschnitt 7.3.2.4 werden elektrische Bedingungen, die sich nicht auf das Fahrzeug beziehen, betrachtet, in Abschnitt 7.3.2.5 solche, die sich auf das Fahrzeug beziehen. Darauf folgt in Abschnitt 7.3.2.6 der Fokus auf den Schutz vor unberechtigtem Zutritt und in Abschnitt 7.3.2.7 die Darstellung von Maßnahmen, die gegen erschwerte Bedingungen nachzuweisen sind. Die verschiedenen Einflüsse werden allgemein betrachtet, da die spezifischen Bedingungen von den Einsatzbedingungen der Ortungseinheit abhängen, die zum jetzigen Zeitpunkt noch nicht feststehen.

7.3.2.1 Klimatische Bedingungen

Für die zu entwickelnde Ortungseinheit ist nachzuweisen, dass sie unter allen Bedingungen des Einsatzgebiets genutzt werden kann. Da das Einsatzgebiet noch nicht bekannt ist, ist zunächst die generische Anwendbarkeit unter den klimatischen Bedingungen Mitteleuropas zu betrachten.

7.3.2.2 Mechanische Bedingungen

Hier wird der Nachweis erbracht, dass das technische System unter normativ gegebenen, spezifischen mechanischen Bedingungen wie einer starken Änderung der Beschleunigung seine geforderten Funktionen sicher erfüllt.

7.3.2.3 Höhe über Meeresspiegel

Für den Nachweis des sicheren Betriebs der Ortungseinheit in allen Höhenlagen des Einsatzgebietes ist deren Kenntnis notwendig. Da das Einsatzgebiet bei der hier

durchgeführten generischen Betrachtung nicht bekannt ist, ist der mögliche Betrieb auf allen normalspurigen Strecken Europas nachzuweisen.

7.3.2.4 Elektrische Bedingungen (nicht auf Fahrzeugen)

In diesem Abschnitt wird die Einhaltung der spezifischen elektrischen Bedingungen betrachtet, die sich nicht auf das Fahrzeug selbst beziehen. Diese Bedingungen sind normativ vorgeschrieben und durch die Ortungseinheit einzuhalten.

7.3.2.5 Elektrische Bedingungen (auf Fahrzeugen)

Hier werden die normativ vorgeschriebenen Bedingungen, unter denen das Fahrzeug sicher funktionieren soll, die sich auf das Fahrzeug beziehen und ebenso einzuhalten sind, betrachtet.

7.3.2.6 Schutz vor unberechtigtem Zutritt

Der Schutz vor unberechtigtem Zutritt ist bedeutend, damit das zu entwickelnde technische System nicht manipuliert werden kann. Dabei sind auf die Definition des Zutrittsniveaus, auf externe Bedingungen und eine notwendige Kapselung zu achten.

7.3.2.7 Erschwerte Bedingungen

Abhängig vom geplanten Einsatzgebiet ist möglicherweise der Betrieb der Ortungseinheit unter erschwerten Bedingungen nachzuweisen. Dies bezieht sich bspw. auf Kondensation, verstärkte Luftverschmutzung, chemische Beeinflussung sowie das Eindringen von Pflanzen und Tieren.

7.3.3 Ausfallauswirkungen

In diesem Abschnitt wird der Nachweis der Ausfallauswirkungen betrachtet, dabei wird in Abschnitt 7.3.3.1 zunächst auf die verwendeten Fail-Safe-Prinzipien eingegangen. In Abschnitt 7.3.3.2 folgt die Darstellung der Unabhängigkeit von Betrachtungseinheiten, die für eine unabhängige Sicherheitsbetrachtung notwendig ist. In Abschnitt 7.3.3.3 wird der Nachweis des Schutzes gegen systematische Fehler als Teil des Entwicklungsprozesses betrachtet, um die Wahrscheinlichkeit eines Unfalls aufgrund dieses Fehlertyps zu reduzieren.

Die nachfolgend genannten Abschnitte befassen sich mit der Auswirkung von Ausfällen auf die Sicherheit der Ortungseinheit. In Abschnitt 7.3.3.4 werden Einzel-, in Abschnitt 7.3.3.5 Mehrfachausfälle fokussiert. Darauf folgen in Abschnitt 7.3.3.6 Aspekte der Offenbarung von Ausfällen mit dem Fokus auf Einzelausfälle sowie in Abschnitt 7.3.3.7 mögliche Reaktionen nach Ausfalloffenbarung.

Bei der Betrachtung von Ausfallauswirkungen liegt der Fokus auf den betrieblichen Gegebenheiten. Zunächst sollten die Sicherheit des Systems und dessen Betrieb darauf ausgerichtet sein, dass keine Fehler auftreten. Falls sie dennoch auftreten, sind diese schnellstmöglich zu erkennen und eine betriebliche Reaktion, bspw. eine Zwangsbremsung, zu veranlassen. Für diese Betrachtung wird die in Abbildung 7-6 eingeführte Anwendung des Modells der Risikogenese genutzt, um Maßnahmen zu ergreifen, damit kein Fehler auftritt. Das in diesem Abschnitt vorgestellte Vorgehen liefert damit einen wesentlichen Beitrag zur Erfüllung der Anforderung an die Ortungseinheit, seine Funktionen jederzeit sicher zu gewährleisten.

7.3.3.1 Angabe der Fail-Safe-Prinzipien

Wesentlicher Bestandteil der in Abbildung 7-6 dargestellten Anwendung des Modells der Risikogenese ist der Übergang in den sicheren Zustand im Fall einer Gefährdung durch entsprechende Fail-Safe-Prinzipien. Der dafür relevante generische Prozess ist in Abbildung 7-7 mit dem Fokus auf den sicheren Zustand dargestellt. Mit diesem Vorgehen soll das Eintreten kritischer Systemzustände generell vermieden werden oder im Falle eines Eintretens möglichst zeitnah eine sicherheitsgerichtete Reaktion erfolgen. Dafür fließen die Betrachtungen der gerätetechnischen Zuverlässigkeit und der messtechnischen Qualität nach [Schnieder 2012] ein. Die gerätetechnische Zuverlässigkeit bezieht sich auf den kritischen technischen Ausfall des Systems, der nicht sofort erkannt oder offenbart wird. Auch bei einem intakten technischen System kann es zu einer nicht korrekten Berechnung der Positionsinformation durch fehlerhafte Sensoreingänge kommen. Daher ist die messtechnische Qualifikation von besonderer Bedeutung. Die Überschreitung bestimmter messtechnischer Grenzwerte ist als Ausfall einzustufen [Schnieder 2012; Lu 2014].

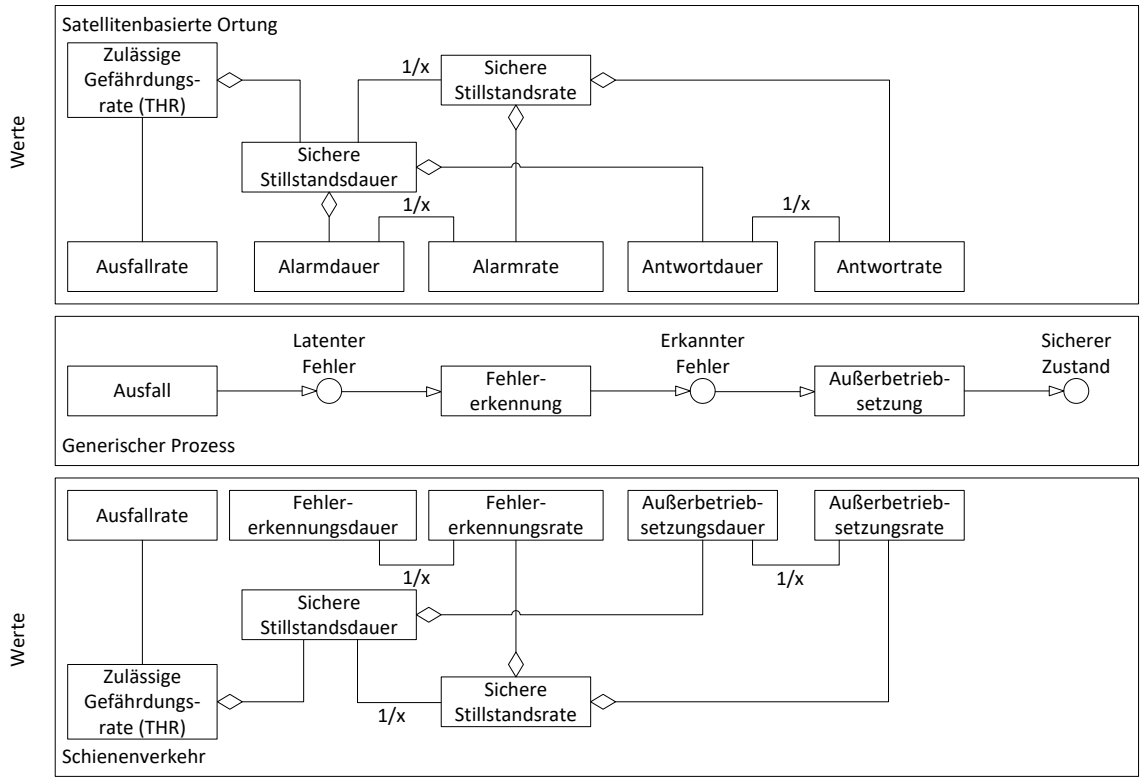


Abbildung 7-7: Generischer Prozess für sicheren Zustand in Schienenverkehr und satellitenbasierter Ortung

Um den sicheren Zustand wiederherstellen zu können, muss der Fehler erkannt werden. Den notwendigen Prozessschritten können dabei Grenzwerte zugeordnet werden, bspw. die THR für die Gesamtzuverlässigkeit des Systems. Nach der Beendigung des Fehlzustands befindet sich das System in einem sicheren Zustand.

Die Fail-Safe-Prinzipien zum Erreichen eines sicheren Zustands sind unverlierbare Eigenschaften, Redundanz und sicherheitsgerichtete Ausfallreaktionen, deren Kombination im weiteren Verlauf dieser Arbeit zur Gewährleistung der Sicherheit der Ortungseinheit genutzt wird. Die Sicherheit des Gesamtsystems soll erreicht werden, indem Ausfälle von einzelnen Komponenten keine sicherheitsrelevanten Folgen haben.

7.3.3.2 Unabhängigkeit von Betrachtungseinheiten

Die Ortungseinheit muss mechanisch, elektromagnetisch und funktional unabhängig von anderen Komponenten des Zugs sein, die nicht für die Ortung oder Zugbeeinflussung zuständig sind. Die Betrachtung der Unabhängigkeit bezieht sich dabei auf physikalische und funktionale Einflüsse, die sowohl intern als auch extern verursacht werden können. Darüber hinaus ermöglicht eine physikalische Unabhängigkeit der Komponenten untereinander deren erhöhte Sicherheit und eine unabhängige Sicherheitsbetrachtung.

Eine diversitäre Entwicklung der Komponenten und Bauteile verhindert zudem, dass der gleiche systematische Fehler in beiden parallelen Elementen gleichzeitig auftritt.

7.3.3.3 Schutz gegen systematische Fehler

Der Schutz gegen systematische Fehler ist notwendig, um die Wahrscheinlichkeit des Eintretens eines Unfalls äußerst gering zu halten und ist daher nachzuweisen. Dies betrifft bspw. Störeinflüsse auf die Sensoren und deren potentielle Fehler, deren Auswirkungen entsprechend der Sicherheitsanforderungen gering gehalten werden sollen. Es muss sichergestellt werden, dass die eingesetzten Sensoren nicht gestört und somit Gegenmaßnahmen zu den möglichen Störungen nach Tabelle 7-2 getroffen werden.

Tabelle 7-2: Mögliche systematische Fehler von Systemkomponenten der satellitenbasierten Ortungseinheit

Systemkomponente	Dynamik	Gemessener Wert	Prinzip	Störung/ Qualität
GNSS-Empfänger	Diskret	s, v	Energetisch	EMV Jamming, Spoofing, Dämpfung, Abschattung, Mehrwegausbreitung
Wirbelstromsensor	Kontinuierlich	s, v, a	Induktiv	EMV Mechanisch
Intertialeinheit	Kontinuierlich		Mechanisch	Mechanisch, Drift
Karte	Diskret		Digital	Nicht exakte Datenübermittlung
Fusion	Diskret		Rechnerisch/ digital	Fehler im Fusionsalgorithmus, Verzögerung durch fehlende Echtzeitverarbeitung
Update	Diskret	Information	Rechnerisch/ digital	Nicht korrekte/ verspätete Lieferung des Updates
Kommunikation		Information	Digital	Unvollständige Übermittlung

Die Systemeigenschaften stehen dabei in engem Zusammenhang zu den geplanten Einsatzbedingungen [Klinge 1998]. Diese beschränken die Entwicklung, da das System nur für definierte Zwecke entwickelt werden kann. Die zur Verfügung stehenden Normen geben für dieses Vorgehen einen sinnvollen Rahmen, die Einsatzbedingungen beschränken die Prüfbedingungen und den Prüfumfang.

7.3.3.4 Auswirkung von Einzelausfällen

Die Auswirkung von Einzelausfällen wird zunächst durch die in Abschnitt 7.3.3.1 eingeführten Fail-Safe-Prinzipien reduziert. Zudem ist mit einer möglichst geringen Ausfallrate der Einzelkomponenten zu gewährleisten, dass Ausfälle selten auftreten. Durch sicherheitsgerichtete Reaktionen auf einen Ausfall wird gewährleistet, dass Ausfälle keine sicherheitsrelevanten Folgen haben, weswegen die Detektion von großer Bedeutung ist. Dies ermöglicht eine Fehlerbeherrschung durch Offenbarung und Diagnose, was wesentlicher Bestandteil der sicheren Systementwicklung ist.

Zur Reduzierung von Einzelausfällen ist eine hohe Qualität der Eingangsinformationen von großer Bedeutung für die Sicherheit des Gesamtsystems. Im Rahmen dieser Arbeit ist dabei die Qualität der durch die GNSS und SBAS zur Verfügung gestellten Informationen wichtig, damit sie als COTS ein sicherer Bestandteil des Gesamtsystems sind. Dafür soll der geplante sichere Dienst von Galileo und EGNOS Integritätsinformationen zur Verfügung stellen. Dieser hat die Aufgabe, den Nutzer über Abweichungen des Signals von der gewünschten Genauigkeit zu informieren. Somit leistet die Eigenschaft Integrität des sicheren Dienstes nach seiner Inbetriebnahme einen wesentlichen Beitrag zur Sicherheit der Ortung, daher sind seine Merkmale, Größen und die zugeordneten Werte mit ihren Einheiten in Abbildung 7-8 dargestellt. Für Fehlererkennungszeit und Außerbetriebsetzungszeit sind keine Werte bekannt.

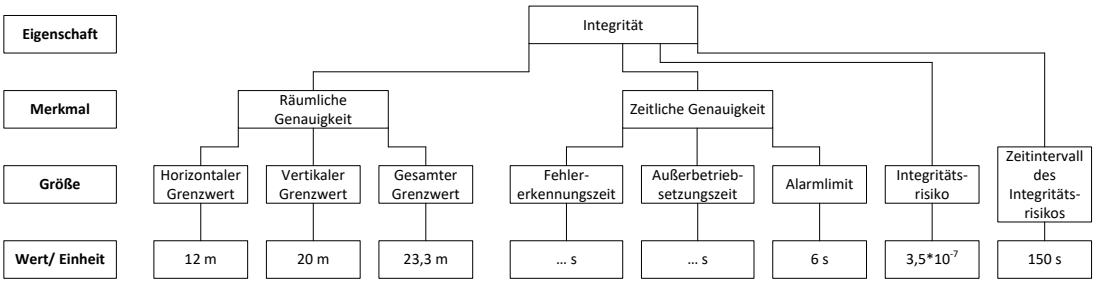


Abbildung 7-8: Attributhierarchie der Integrität [EC/ESA 2002]

Die Integritätsinformation wird mit einer Wahrscheinlichkeit von $3{,}5*10^{-7}$ in 150 Sekunden nicht korrekt zur Verfügung gestellt. In der Terminologie der Spezifikation wird dieser Aspekt als Integritätsrisiko bezeichnet. Die Übertragung der sehr ähnlichen Gefährdungsrate des Anflugverfahrens mit vertikaler Führung (APV) der ICAO ($2*10^{-7}$ in 150 Sekunden) in die Terminologie des Schienenverkehrs wurde in [Lu et al. 2012] und [Lu 2014] durchgeführt. Durch eine Monte Carlo Simulation eines stochastischen Petrinetzes wird die Gefährdungsrate mit $4{,}77*10^{-6}$/h abgeschätzt. Somit kann angenommen werden, dass die Integritätsinformationen durch den sicheren Dienst von Galileo mit einer Wahrscheinlichkeit von etwa $5*10^{-6}$/h nicht korrekt zur Verfügung gestellt werden. Die angegebenen Genauigkeiten stehen dem Nutzer zur Verfügung. Zum TTFF benötigen Empfänger gewöhnlich 18 bis 36 Sekunden [Zogg 2009].

7.3.3.5 Auswirkung von Mehrfachausfällen

Die in Abschnitt 7.3.3.4 dargestellten Aspekte bezüglich Einzelausfällen haben für Mehrfachausfälle ebenso Gültigkeit, wobei Mehrfachausfälle schwerwiegendere Auswirkungen haben und somit einer höheren Aufmerksamkeit bedürfen. Daher ist es von besonderer Bedeutung, den sicheren Zustand innerhalb kürzester Zeit herzustellen. Bei Mehrfachausfällen ist die Detektion erschwert, insbesondere wenn zwei gleiche

redundante Komponenten ausfallen. Dies gilt speziell bei einem vergleichbaren Fehler und ähnlich fehlerhaften Werten. Bei dieser – äußerst unwahrscheinlichen – Konstellation könnte nicht, wie sonst bei einer Redundanz üblich, der Fehler einer Komponente durch die funktionsfähige, baugleiche Komponente erkannt werden.

Das Nichterkennen von Fehlern, was durch Redundanz verhindert werden sollte, trifft zudem bei Sensoren ein, welche auf die gleichen externen Daten zugreifen, bspw. auf ein GNSS. Wenn Sensoren Ihre Position nur aufgrund von GPS-Informationen berechnen und GPS fehlerhaft ist, kann der Fehler zunächst nicht erkannt werden. Somit ist für die Berechnung der Ortungsinformation die Nutzung mehrerer GNSS und dadurch die Unabhängigkeit der Eingangsinformationen notwendig.

7.3.3.6 Offenbarung von (Einzel-)Ausfällen

Zur sicheren Funktionalität eines technischen Systems ist die Offenbarung von Ausfällen von Bedeutung, wozu zunächst sicherheitsrelevante von nicht sicherheitsrelevanten Systemen getrennt werden sollten. Für die genutzte Hardware sind quantitative Zuverlässigkeitsanalysen notwendig, auf deren Basis die Systemarchitektur begründet erstellt wird [DIN EN 50126].

7.3.3.7 Aktion nach Ausfalloffenbarung

Die Offenbarung eines Ausfalls sollte zu einer schnellen Reaktion führen, um innerhalb kürzester Zeit einen sicheren Zustand herbeizuführen. Weitere Ausfälle dürfen nicht zum Verlassen des sicheren Zustands führen [DIN EN 50126].

7.3.4 Nachweis des korrekten funktionalen Verhaltens

Der Nachweis des korrekten funktionalen Verhaltens der Ortungseinheit ist für deren Zertifizierung notwendig, in diesem Abschnitt werden die Besonderheiten aufgrund der innovativen Nutzung der satellitenbasierten Ortung als COTS fokussiert. Dabei wird in Abschnitt 7.3.4.1 zunächst auf die zu erfüllenden Sicherheitsanforderungen eingegangen, in Abschnitt 7.3.4.2 auf den Nachweis der korrekten Hardwarefunktionalität und in Abschnitt 7.3.4.3 auf den Nachweis der korrekten Softwarefunktionalität. Mit diesem Vorgehen wird der Einsatz der Ortungseinheit auf Regionalstrecken ermöglicht. Um zukünftig eine möglichst generische Anwendbarkeit zu ermöglichen, ist auch eine Aufwärtskompatibilität für den Einsatz auf anderen, beliebigen Streckenkategorien zu berücksichtigen.

7.3.4.1 Erfüllung der Sicherheitsanforderungen

Die Wahrscheinlichkeit des Eintretens eines Schadens und dessen Ausmaß können sich entsprechend der gefahrenen Zugkilometer und des betrachteten Streckenabschnitts unterscheiden. Das kann bei unterschiedlichen Verfügbarkeiten der satellitenbasierten Ortung oder angrenzenden Strecken, die ein zusätzliches Risiko verursachen, der Fall sein. Daher kann sich der Sicherheitsnachweis, wenn er nicht für das höchstmögliche Risiko durchgeführt wird, nach der geplanten Streckenkategorie unterscheiden.

Zum Erfüllen der Sicherheitsanforderungen aus Kapitel 6 können Gefährdungen identifiziert werden, die zu einem unerwünschten Zustand führen können, um diesen durch risikoreduzierende Maßnahmen zu begegnen. Nachteilig bei diesem Vorgehen ist, dass unter Umständen nicht alle unerwünschten Zustände und nicht alle Ursachen erkannt werden. In diese Betrachtung sind alle potentiellen Umwelteinflüsse einzubeziehen.

Die Gefährdungsanalyse des Systems und dessen Komponenten soll auf Basis der angestrebten THR von $< 10^{-8}\ h^{-1}$, was SIL 3 entspricht, durchgeführt werden, um die Implementierung in ETCS Level 3 zu ermöglichen. Generell hängt das zu erreichende SIL von den betrieblichen Bedingungen der Einsatzstrecke ab, weswegen die Strecke und auftretende besondere Unfalltypen ebenso zu betrachten sind. Da der Einsatz der Ortungseinheit als Teil eines Zugbeeinflussungssystems angestrebt wird, wird das dort gebräuchliche SIL als Referenzrisiko genutzt. Diese Betrachtung ist Teil der Anforderungen und somit auch der Spezifikationen, auf denen die Entwicklung aufbaut. Aufgrund der angestrebten Nutzung der Ortungseinheit in allen Ländern Europas ist eine Anerkennung der in einem Land – bspw. Deutschland – erteilten Zertifizierung in weiteren europäischen Ländern angebracht und erstrebenswert.

Zum Nachweis der sicheren Bestimmung der Geschwindigkeit und der gefahrenen Strecke ist ein formaler Nachweis zu führen. Zudem sollten sichere Reaktionen auf spezifische Szenarien festgelegt und der Nachweis des Ausbleibens von systematischen Fehlern geführt werden. Ein bedeutender Beitrag zum Erreichen der Sicherheit und Verlässlichkeit der Ortungseinheit ist die Struktur der Komponenten und Sensoren. Dabei können einfache oder redundante Strukturen genutzt werden. Einfache Strukturen umfassen serielle und parallele Systeme oder eine Kombination aus beiden. Redundante Strukturen können vielfältig erreicht werden, bspw. durch Vergleichersysteme (nvn-Systeme) oder Mehrheitsentscheidungssysteme (mvn-Systeme) [Fricke/Piereck 1990] sowie durch aktive und passive Redundanz, Softwareredundanz oder Hardwareredundanz.

Für den Nachweis der mindestens gleichen Sicherheit im Vergleich zum bestehenden System sind die Analyse der Funktionen und deren jeweiliger Gefährdungen notwendig. Die klassifizierten Sicherheitsfunktionen des alten und neuen Systems werden gegenübergestellt und Maßnahmen zur Risikoreduktion getroffen [Drewes 2009]. Für die Anwendungsfälle einer Funktion werden zunächst qualitativ Fehler sowie deren Ursachen und Auswirkungen zugeordnet. Mit einer anschließenden quantitativen Risikoklassifikation wird nachgewiesen, dass von den sicherheitsrelevanten Funktionen weder systematische noch zufällige Fehler ausgehen [DIN EN 50126]. Bei der Sicherheitsnachweisführung wird bewertet, ob das Risiko des betrachteten Systems auf ein akzeptables Niveau gesenkt wird.

Zum vergleichenden Nachweis der Sicherheit sollte ein vergleichbares, auf der gleichen Streckenkategorie genutztes Zugbeeinflussungssystem dienen. Auf bestehenden eingleisigen Nebenstrecken mit einfachen betrieblichen Verhältnissen mit einer Streckenhöchstgeschwindigkeit von 80 km/h ist das angewandte Betriebsverfahren der Zugleitbetrieb [Scheppan 2006] gemäß [DB Ril 436]. Aufgrund des Fokus dieser Arbeit auf Nebenstrecken mit geringer Zugfolge wird der dort gebräuchliche Zugleitbetrieb als Referenzsystem gewählt.

Für den Vergleich von Zugbeeinflussungssystemen in dieser Arbeit wird lediglich der Zusammenstoß, also die Schutzfunktionen Folgefahrschutz, Gegenfahrschutz und Flankenschutz, und die Überwachung der Höchstgeschwindigkeit als relevant angesehen. Auf alle anderen Schutzfunktionen und daraus resultierende Risiken hat die Migration des Zugbeeinflussungssystems keinen Einfluss. Aufgrund der schwierigen Verfügbarkeit von statistischen Daten wird in [Weber 2010] der energetische Ansatz unter Einbeziehung der menschlichen Fehlerrate nach [Hinzen 1993] zur Betrachtung gewählt. Aus den möglichen Fehlern, die beim Zugleitbetrieb auftreten können (Zugleiter irrt sich in der Ausgabe einer Fahrerlaubnis; Zugleiter und Triebfahrzeugführer irren sich in Herausgabe einer Fahrerlaubnis; Triebfahrzeugführer glaubt eine Fahrerlaubnis erhalten zu haben, obwohl das nicht der Fall ist) ergibt sich nach [Weber 2010] eine Fehlerrate von 0,001011 $^{1}/_{h}$. Mit veränderter Anzahl der Züge auf einer Strecke verändert sich auch die Fehlerrate, jedoch gibt diese Berechnung eine grobe Größenordnung für die Fehlerrate des Zugleitbetriebs. Da diese Fehlerrate wesentlich höher als das angestrebte SIL 3 ist, wird davon ausgegangen, dass SIL 3 die Sicherheit erhöht und somit ein sinnvolles Sicherheitsziel für diese Arbeit darstellt. Die Analyse der Testspezifikationen und Sicherheitsanalysen schließt den Nachweis der Erfüllung der Sicherheitsanforderungen ab.

7.3.4.2 Nachweis der korrekten Hardwarefunktionalität

Der Nachweis der korrekten Hardwarefunktionalität beinhaltet insbesondere die Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit und Sicherheit (RAMS) der Systemkomponenten [DIN EN 50126]. Die hier zu zertifizierende Hardware lässt sich in solche, die entsprechend des normativen Rahmens des Schienenverkehrs und solche, die nicht für den Schienenverkehr zertifiziert wurde, unterteilen. Für den Schienenverkehr zertifiziert wurden bspw. der sichere Rechner und eine Mensch-Maschine-Schnittstelle. Nicht im Schienenverkehr zertifiziert wurden COTS wie bspw. die digitale Karte, das Hodometer und der GNSS-Empfänger. Dieser Zusammenhang ist schematisch in Abbildung 7-9 dargestellt. Auf die bereits im Schienenverkehr zertifizierten Komponenten wird im Folgenden nicht weiter eingegangen, da lediglich eine Integration über Schnittstellen notwendig ist.

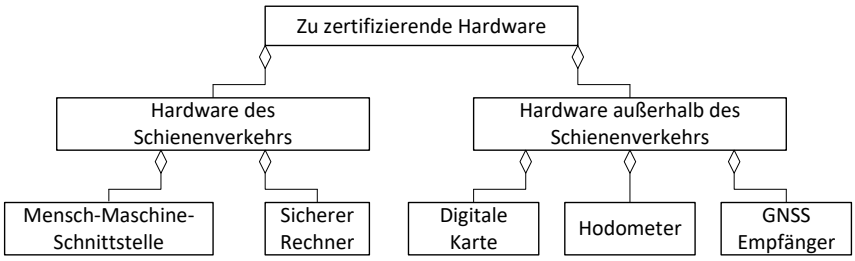


Abbildung 7-9: Zu zertifizierende Komponenten der satellitenbasierten Ortungseinheit

Zum Nachweis der korrekten Hardware-Funktionalität sind sowohl Sicherheit als auch Verfügbarkeit zu betrachten. Der Stillstand ist im Schienenverkehr ein sicherer Zustand, er sollte jedoch möglichst selten genutzt werden. Zur Integration von COTS in dieser Arbeit sind verschiedene Ansätze möglich:

1. Externe Zertifizierung und Dokumentation des Herstellers (Originalausrüstungshersteller – OEM) entsprechend der Normung des Schienenverkehrs
2. Erklärung des Herstellers, dass sein Produkt anderen sicherheitsrelevanten Industrienormen, bspw. denen der Luftfahrt, entspricht und Vergleich mit normativem Rahmen des Schienenverkehrs
3. Gesonderte Qualifikation der COTS
4. Garantieerklärung und Versicherung des Herstellers der COTS
5. Zusätzliche Anforderungen des Käufers/ Nutzers, die vom Komponentenhersteller bestätigt werden

Wenn einer der fünf aufgezählten Punkte nicht mit den Voraussetzungen der Anwendung übereinstimmt, müssen durch den Hersteller oder Nutzer entsprechende Anpassungen

vorgenommen werden. Im ersten dargestellten Ansatz muss die Zertifizierung durch die Sicherheitsbehörden mit cross-acceptance akzeptiert werden.

Im zweiten Ansatz muss zunächst die Kompatibilität der verwendeten Normen mit der Normung im Schienenverkehr nachgewiesen werden. Dieser Ansatz ist möglicherweise auf den GNSS-Empfänger anwendbar, da dessen sicherheitsrelevante Nutzung in der Luftfahrt vorgesehen ist. Die gegenseitige Anerkennung muss in diesem Fall für die Verwendung eines Produkts aus einer anderen Domäne durchgeführt werden. Somit muss sichergestellt werden, dass das Produkt in der anderen Domäne gemäß solchen Normen, welche mit denen im Schienenverkehr vergleichbar sind, zertifiziert wurde. Der erste und zweite Ansatz können dabei auch basierend auf bestehenden Prozessen unter Berücksichtigung der Produkthaftung durchgeführt werden. Der dritte Ansatz der gesonderten Qualifikation der COTS ist eine domänenübergreifende gegenseitige Anerkennung ohne die Verfügbarkeit von Normen mit Nutzung der verfügbaren Dokumentation. Dies hätte zur Folge, dass eigene Kriterien für die Qualifizierung der Messungen, Prozesse und Tests erstellt werden müssten [Wegener 2013; Spiegel et al. 2014; Spiegel/Becker 2015].

7.3.4.3 Nachweis der korrekten Softwarefunktionalität

Beim Nachweis der korrekten Softwarefunktionalität sind die Abhängigkeiten zwischen Hard- und Software sowie die Reihenfolge deren Zusammenwirkens zu beachten. Zudem sind die Antwortzeiten sowie Selbsttests von Bedeutung [DIN EN 50126].

Die Software der satellitenbasierten Ortung ist so zu konzipieren, dass sie kontinuierlich die signaltechnisch sichere Bestimmung der Position des Zuges in Echtzeit ermöglicht. Diese Anforderung ergibt sich aus dem quantitativen Sicherheitsziel des Betreibers und den normativen Sicherheitsanforderungen. Da die Position des Zuges, unabhängig von der Ortungsmethode, nie exakt bestimmt werden kann, liegt diese in einem sicherheitsrelevanten Konfidenzintervall, welches von der geforderten Genauigkeit der Ortungsmethode abhängt. Das veränderliche Konfidenzintervall bezieht sich dabei auf betriebliche Bedingungen wie die Genauigkeit längs zur Fahrtrichtung, die Genauigkeit senkrecht zur Fahrtrichtung ist davon nicht betroffen – eine gleisselektive Ortung ist dennoch zu jedem Zeitpunkt zu gewährleisten. Die zu erzielende Genauigkeit längs zur Fahrtrichtung ist von den örtlichen Gegebenheiten abhängig, bspw. ist in der Umgebung von Weichen, Bahnübergängen oder im Bahnhofsbereich eine höhere Genauigkeit, also ein geringeres Konfidenzintervall, sinnvoll. Auf der freien Strecke bei ausreichender Entfernung zu Gefährdungspunkten kann ein höheres Konfidenzintervall akzeptiert

werden. Ein festes (hohes) Konfidenzintervall würde an kritischen Stellen zu hohe Ungenauigkeiten verursachen.

„Ein sicherheitsrelevantes Vertrauensintervall [sic] ist ein Intervall, in dem sich der wahre Wert eines Prozesszustands mit signaltechnischer Sicherheit gemäß dem Schutzziel befindet“ [Kiriczi 1996], es ist durch Mittelwert und die jeweilige Halblänge des sicherheitsrelevanten Vertrauensintervalls [sic] definiert. Die zu erstellenden Vorschriften zur Berechnung des Vertrauensintervalls sind mit den Vorschriften der Zertifizierung in Einklang zu bringen. Zudem sind Vorschriften für die Entwicklung des Systems, den Betrieb sowie die Wartung zu beachten bzw. zu erstellen. Ebenso von Bedeutung ist der zulässige Einsatz des zu entwickelnden Systems. Eine Entwicklung des Systems für alle weltweiten Schienenverkehrsstrecken kann unter Umständen zu einem unverhältnismäßigen Entwicklungsaufwand führen, der durch einen fokussierten Einsatzbereich des Systems klar begrenzt und definiert wird. Dies stellt den Entwickler vor ein gewisses Dilemma, da ein möglichst breit gefasster Einsatzbereich die Anwendungs- und somit auch Verkaufsmöglichkeiten des Systems vergrößert, bei einem größeren Einsatzbereich jedoch auch der Entwicklungsaufwand entsprechend steigt. Weiterhin muss der Schutz gegen Manipulation gewährleistet sein sowie Anforderungen an Bedienung, Hard- und Softwaresicherheit abgedeckt sein.

Das einzuhaltende Sicherheitsziel in Form einer THR für das Gesamtsystem ist durch die Kombination der Gefährdungsraten der Teilsysteme einzuhalten. Dabei fließen alle für das Gesamtsystem relevanten Faktoren ein, diese sind bspw. Gefährdungen in Betrieb und Wartung, unzulässiger Einsatz, Manipulation oder Fehlbedienung. Durch die Software ist weiterhin zu gewährleisten, dass unzulässige Betriebszustände zu einer sicheren Reaktion führen, damit das System keine unzulässigen Werte ausgibt. Dies wird in Tests erprobt, die in Abschnitt 7.3.6 betrachtet werden.

7.3.5 Sicherheitsbezogene Anwendungsbedingungen

Sicherheitsbezogene Anwendungsbedingungen sind notwendig, falls im Systementwurf nicht für alle Funktionen und Anwendungsfälle die Sicherheit gewährleistet werden kann. Damit kann trotz geringer Defizite im Systementwurf die Sicherheit des Gesamtsystems gewährleistet werden. Sicherheitsbezogene Anwendungsbedingungen sind bspw. für die Ausrüstung, den Betrieb und die Instandhaltung, wie in Abschnitt 7.3.5.1 dargestellt, aufzustellen. Weiterhin kann eine Sicherheitsüberwachung im Betrieb notwendig sein, was in Abschnitt 7.3.5.2 betrachtet wird. Auch ist die Stilllegung und Entsorgung zu betrachten, für die spezielle Bedingungen in Abschnitt 7.3.5.3 aufgestellt werden.

7.3.5.1 Betrieb und Instandhaltung

Während des Betriebs und der Instandhaltung eines technischen Systems ist eine Vielzahl von Aspekten zu betrachten. Für besonders seltene Situationen bietet sich das Aufstellen von sicherheitsbezogenen Anwendungsbedingungen an. Diese können den Betriebszustand, Instandhaltungsstufen, eine eventuell notwendige periodische Instandhaltung und zu verwendende Instandhaltungshilfen umfassen.

Nach Abschluss der sicherheitsgerichteten Systementwicklung liegt ein normativ und legislativ sicheres System vor. Die Sicherheitsbetrachtung ist zur Erhöhung der Sicherheit während des Betriebs durch betriebliche Maßnahmen fortzusetzen. Zudem kann die reale bzw. objektive Sicherheit eines Systems erst im Betrieb statistisch bestimmt werden und stimmt unter Umständen nicht mit der vorher analytisch ermittelten Sicherheit überein. Ein Abgleich der analytisch berechneten Sicherheit und der statistisch im realen Betrieb bestimmten Sicherheit erscheint sinnvoll, um diesem Sachverhalt mit einer sicherheitsbezogenen Anwendungsbedingung und einer Weiterentwicklung des Systems zu begegnen. Bei der Unfallanalyse sollten auch Beinaheunfälle berücksichtigt werden, deren Häufigkeit kann ein Indikator zum Vergleich sein. Mittelwerte sollten generell über einen langen Zeitraum von mehreren Jahren gebildet werden.

Um Rückschlüsse zwischen analytisch bestimmter und statistischer Sicherheit zu ermöglichen, ist eine Unfallanalyse nach jedem Unfall notwendig. Dabei sollten nicht nur die rechtlichen Verantwortlichkeiten geklärt sondern auch die Ursachen betrachtet werden. Ein besonderes Augenmerk sollte darauf gelegt werden, ob der Unfall trotz einer Entwicklung nach dem Stand der Technik aufgetreten wäre.

7.3.5.2 Sicherheitsüberwachung im Betrieb

Zur Gewährleistung der Sicherheit während des Betriebs eines technischen Systems ist neben den bereits dargestellten Maßnahmen die Sicherheit zu überwachen. Dies schließt die Überwachung der sicherheitsrelevanten Leistungsfähigkeit sowie die Überprüfung der während des Betriebs generierten Fehlerberichte ein. Zudem sind die Berichte über Zwischenfälle und Unfälle im Detail zu analysieren, um so Rückschlüsse für eine Verbesserung des Betriebsablaufs ziehen zu können. Dabei sind auch kleine, auf den ersten Blick möglicherweise unwesentliche Zwischenfälle zu betrachten, da auch daraus Verbesserungen des Betriebsablaufs abgeleitet werden können.

7.3.5.3 Stilllegung und Entsorgung

Vorkehrungen für die Stilllegung und Entsorgung eines Fahrzeugs sind nicht Bestandteil dieser Arbeit, sie sind dennoch als Teil der technischen Sicherheitsvorkehrungen zu dokumentieren. Dabei sollten für alle Phasen der Einführung und des Betriebs des Fahrzeugs notwendige und geeignete Warnungen und Hinweise enthalten sein.

7.3.6 Sicherheitserprobung

Die Sicherheitserprobung ist vor Inbetriebnahme eines jeden Systems im Schienenverkehr und somit auch bei der hier betrachteten Ortungseinheit durchzuführen. Die Grundlagen für die Überprüfung der sicheren Funktionalität wurden in den in Abschnitt 6.4 erstellten Anforderungen an die Sicherheitserprobung dargestellt. In Abschnitt 7.3.6.1 werden zunächst notwendige Schritte zur Erfüllung der Systemanforderungen betrachtet, in Abschnitt 7.3.6.2 wird Bezug zu den Ergebnissen der Sicherheitserprobung genommen.

7.3.6.1 Erfüllung der Systemanforderungen

Zum Nachweis der Erfüllung der Systemanforderungen werden zunächst die Entwurfsprinzipien und deren Berechnung betrachtet. Zudem sind Testspezifikationen zu erstellen, um entsprechende Testergebnisse zu erhalten. Weiterhin erfolgt eine Validierung der Entwicklung, es wird somit untersucht ob die Eigenschaften des Systems im Realbetrieb mit den gestellten Spezifikationen übereinstimmen [DIN EN 50126].

Zur Prüfung der sicheren Funktionalität der satellitenbasierten Ortungseinheit müssen die Spezifikationen und Anforderungen an das betrachtete System, hier die Ortungseinheit, im Blick behalten werden. Im Hauptfokus steht dabei die Generierung einer sicheren Position durch die korrekte Verarbeitung unsicherer Eingangsdaten und deren Kombination mit sicheren Informationen bzw. in einer sicheren Rechnerstruktur.

Im Fall der in dieser Arbeit betrachteten satellitenbasierten Ortungseinheit sind die korrekte Funktionalität der technischen Spezifikationen der Ortungseinheit, des Ortungsalgorithmus des Wirbelstromsensors und des GNSS-Empfängers sowie der digitalen Karte und des zugehörigen Map-Matching-Algorithmus nachzuweisen.

Die Qualität ist eine Eigenschaft von höchster Bedeutung für ein sicherheitsrelevantes System und kann dabei in verschiedene Aspekte wie die Messabweichung gegliedert werden [DemoOrt 2009; Wegener et al. 2011]. Zur Untersuchung der Qualität der Ortungseinheit kann während der Sicherheitserprobung ein Referenzmesssystem genutzt

werden [DemoOrt 2009; Wegener et al. 2010; Wegener/Schnieder 2013; Wegener 2013]. Das bietet die Möglichkeit, die Einhaltung geforderter Größen und damit die Qualität satellitenbasierter Ortungssysteme zu evaluieren und zu analysieren [Grasso Toro et al. 2012]. Als weitere Testmöglichkeit bietet sich bspw. das RailGate an, bei dem die GNSS-Empfangseigenschaften unter simulierter Galileo-Umgebung getestet werden können [Engelhardt et al. 2011].

Durch dieses Vorgehen kann analysiert werden, ob die Ortungseinheit kontinuierlich, lediglich im Rahmen der THR, falsche oder fehlerhafte Positionsinformationen weitergibt. Es kann also untersucht werden, ob eine sichere Berechnung erfolgt und mögliche Fehler offenbart werden. Dafür ist auch die Aktualität der verwendeten Informationen zu analysieren. Das betrifft die digitale Karte, deren Aktualisierung bezüglich baulicher Veränderungen oder kurzfristig notwendiger Maßnahmen sicherzustellen ist. Auch muss sichergestellt werden, dass die eingehenden Sensordaten, die fusioniert werden sollen, korrekt sind, um fehlerfrei verarbeitet werden zu können.

7.3.6.2 Ergebnisse

Nach Abschluss der Sicherheitserprobung sind die durchgeführten Tests und deren Ergebnisse mit einem Bericht vollständig zu beschreiben.

7.4 Zusammenfassung und Schlussfolgerung

Im Abschnitt „Zusammenfassung und Schlussfolgerungen“ des technischen Sicherheitsberichts werden zunächst Verbindungen zu anderen Sicherheitsnachweisen und weiteren relevanten Dokumenten mit Sicherheitsbezug hergestellt. Weiterhin wird der technische Sicherheitsbericht resümiert, bspw. bezüglich der Zielerreichung oder Konsequenzen für Entwicklungen anderer, vergleichbarer Systeme.

In diesem Abschnitt wird die Zusammenfassung und Schlussfolgerung der technischen Sicherheitsanalyse und Umsetzung dargestellt. Dabei werden in Abschnitt 7.4.1 kurz die Beziehungen zu anderen Sicherheitsnachweisen betrachtet, in Abschnitt 7.4.2 wird eine abschließende Zusammenfassung gegeben.

7.4.1 Beziehungen zu anderen Sicherheitsnachweisen

Als Teil der Zusammenfassung sind Beziehungen zu anderen Sicherheitsnachweisen anzugeben. Damit werden bereits durchgeführte Begutachtungen und somit der Verweis zum Stand der Technik deutlich.

7.4.2 Zusammenfassung

Nach Abschluss der sicherheitsgerichteten Entwicklung, welche durch den technischen Sicherheitsbericht dokumentiert wird, folgt der Antrag auf Typzulassung durch die Sicherheitsbehörde [VV NTZ ÜGR Stufe 2 2013]. Dabei ist der Grund für die Beantragung einer Inbetriebnahmegenehmigung oder Nutzungsgenehmigung für die betreffende (Signal-)Anlage anzugeben. Zudem sind Abweichungen und Änderungen zu bestehender, bereits zertifizierter Technik darzustellen. Die hohe Sicherheitsverantwortung des EVU, die in der Vergangenheit gestiegen ist [Leining 2014], wird hier durch seine Zuständigkeit für die sichere Abwicklung des Schienenverkehrs deutlich. Außerdem kann der Hersteller für das Schienenfahrzeug oder Teile eine Zertifizierung beantragen [EU/2009/352], so zertifizierte Systeme können durch mehrere Betreiber genutzt werden, was insbesondere für kleinere Betreiber von Vorteil ist.

Für den Antrag auf Typzulassung sind verschiedene Dokumente einzureichen – Anforderungsspezifikationen, Sicherheitsplan, Bewertungsdokumentation sowie Prüferklärungen. Die Prüferklärungen haben dabei Bezug auf die beabsichtigte Nutzung und somit die Eignung für die im Pflichtenheft enthaltenen Anforderungen zu nehmen [VV NTZ ÜGR Stufe 2 2013]. Zusätzlich ist die Einhaltung des für den Begutachtungsgegenstand relevanten normativen Rahmens sowie die Vollständigkeit und Unabhängigkeit des Gutachtens zu betrachten. Nach Prüfung der Antragsunterlagen erfolgt die Typzulassung durch das EBA für den Einsatz durch den Betreiber. Die Typzulassung kann dabei mit Nebenbestimmungen verbunden sein.

Im folgenden Kapitel 8 wird der Blick des Gutachters auf den Begutachtungsgenstand, also die erarbeitete Dokumentation, betrachtet.

8 Sicherheitsgutachten

Nach der sicheren Systementwicklung ist dessen Begutachtung auf Basis des in Kapitel 7 dargestellten Sicherheitsnachweises notwendig, um die sichere Funktionalität zu bestätigen, was schließlich eine Zertifizierung ermöglicht. Dabei wird analysiert, ob die in den Kapiteln 5 und 6 erarbeiteten Anforderungen eingehalten wurden.

Das Sicherheitsgutachten wird von einem akkreditierten Gutachter entsprechend den ihm zur Verfügung stehenden Dokumenten des Begutachtungsgegenstands, seinen Erkenntnissen aus Audits und entwicklungsbegleitenden Gesprächen erstellt. Zur Analyse des zu begutachtenden technischen Systems kann eine funktionsbasierte, datenorientierte, ereignisbasierte oder objektorientierte Dekomposition genutzt werden. Während der Analysephase ist es üblich, verschiedene Arten der Dekomposition zu mischen, um ein möglichst vollständiges und lückenloses Modell zu erhalten. Zudem ist die Verfügbarkeit des Gesamtsystems in die Betrachtung einzubeziehen. Diese Verfügbarkeit kann in die Kategorien politisch, zeitlich, technisch und betrieblich unterteilt werden.

Für die Betrachtung des Sicherheitsgutachtens in diesem Kapitel wird in Abschnitt 8.1 zunächst der Begutachtungsgegenstand dargestellt. In Abschnitt 8.2 wird die bedeutende Unabhängigkeit des Gutachters dargestellt, darauf aufbauend wird in Abschnitt 8.3 die Durchführung der Begutachtung betrachtet. In Abschnitt 8.4 werden Inhalte der durch den Gutachter durchzuführenden Dokumentation dargestellt. Maßnahmen, die bei der Abweichung von aufgestellten Sicherheitsanforderungen durchzuführen sind, werden in Abschnitt 8.5 fokussiert.

8.1 Begutachtungsgegenstand

Der Begutachtungsgegenstand ist die entwicklungsbegleitende Dokumentation des technischen Systems, in dieser Arbeit somit inklusive COTS-Systemen und Grundlage jeder Begutachtung. Der Sicherheitsnachweis muss vollständig sein, da sonst davon ausgegangen wird, dass die Entwicklung unvollständig ist.

8.2 Unabhängigkeit des Gutachters

Der Gutachter soll unabhängig von an der Entwicklung beteiligten Institutionen wie Entwickler, Hersteller, Lieferant, Monteur, Besteller, Betreiber, Eigentümer und Instandhalter sein. Er führt die Begutachtung eigenverantwortlich durch. Die Unabhängigkeit ist ebenso durch die beteiligten DeBo, NoBo und AssBo sicherzustellen.

Der Gutachter bietet dem Entwicklungsprozess seine Fachkompetenz bezüglich der Gültigkeit, Verständlichkeit und Akzeptanz der Argumente und Beweise basierend auf den der Entwicklung und Begutachtung zugrunde liegenden normativen Dokumenten. Die Aufgabe des Gutachters ist es dabei, die Projektdokumentation, die ihm vom Anwender oder Hersteller zur Verfügung gestellt wird, kritisch zu überprüfen, um die Anwendbarkeit des Produkts zu beurteilen. Der Gutachter hinterfragt dabei, ob die Übereinstimmung mit den Anforderungen mit einer passenden und ausreichenden Prüfung sowie Tests analysiert wurde. Weiterhin wird untersucht, ob vernünftig praktizierbare Kontroll- und Schadensminderungsmaßnahmen eingeführt wurden, um Risiken zu begegnen, die von den identifizierten Gefährdungen ausgehen.

Die Begutachtung erfolgt bezüglich der Verlässlichkeit einschließlich Sicherheit, Verfügbarkeit und Instandhaltbarkeit des technischen Systems unter den gegebenen Umweltbedingungen bei Kompatibilität mit der geplanten Infrastruktur. Der Begutachtungsgegenstand sollte dafür eine angemessene Dokumentation bezüglich Entwurf, Test, Installation, Ausbildung des Personals, Betrieb, Instandhaltung und ggf. Entsorgung darstellen. Dies beinhaltet die korrekte Dokumentation der Hard- und Softwareschnittstellen.

8.3 Durchführung der Begutachtung

Die in diesem Abschnitt betrachtete Durchführung der Begutachtung startet bereits projektbegleitend [Schnieder/Schnieder 2013]. Der Gutachter betrachtet als Grundlage für die behördliche Zertifizierung, ob im Begutachtungsgegenstand (Abschnitt 8.1) das gestellte Sicherheitsziel mit der Systementwicklung nachweisbar erreicht und entsprechend dokumentiert wurde. Dabei muss zwischen den technischen und funktionalen Komponenten unterschieden werden. Die Funktionen können einer oder mehreren Komponenten zugeordnet werden.

Die Begutachtung und somit auch die vorangehende Sicherheitsnachweisführung müssen projektspezifisch durchgeführt werden. Zertifizierungen von Teilsystemen oder Komponenten können genutzt werden, wenn sie begründet angepasst werden. Auch die verwendeten Dokumente, aus denen bspw. Anforderungen oder Spezifikationen abgeleitet werden, sind als Quelle der Begutachtung im Gutachten zu referenzieren. Für den Fall, dass während der Begutachtung offene Punkte der Produktentwicklung aufgetan werden, können im Gutachten sicherheitsbezogene Anwendungsbedingungen aus dem Validationsbericht und dem Sicherheitsnachweis aufgestellt werden, deren Erfüllung für eine sichere Funktionalität des Systems notwendig ist. Zudem können im Gutachten Vorschläge zur Behebung der offenen Punkte gegeben werden.

Zur Begutachtung der Entwicklung und seiner Dokumentation wie Qualitäts- und Sicherheitsmanagement des Herstellers, bietet sich eine Vor-Ort Begutachtung an, um einen detaillierten Einblick in das Arbeits- und Entwicklungsumfeld zu erhalten. Damit lassen sich die gültigen Prozesse im Detail analysieren. Nach Verständnis des Qualitäts- und Sicherheitsmanagements des Herstellers können die darauf aufbauenden Dokumente besser eingeordnet werden. Von Vorteil für den Gutachter und für die Implementierung der Prozesse ist ein Qualitätsmanagement des Herstellers, welches leicht für die Mitarbeiter zugänglich ist, bspw. durch eine Dokumentation im Intranet.

Zudem sollten die zur Projektentwicklung verwendeten Dokumente sinnvoll und nachvollziehbar versioniert sein, um hier eine Nachvollziehbarkeit für die Entwickler und für die Begutachtung zu ermöglichen. Die Versionierung kann einerseits durch eine dafür geeignete Software, anderseits durch klar definierte Regeln realisiert werden. Die Versionierungsliste sollte in den Dokumenten enthalten sein, auch sollte ein Zugriff auf ältere Versionen und nicht mehr gültige Dokumente möglich sein, um eine Nachvollziehbarkeit zu gewährleisten.

8.4 Dokumentation der Begutachtung

Ergebnis der Begutachtung ist ein widerspruchsfreies Gutachten des Gutachters, mit dem der Hersteller gegenüber der Sicherheitsbehörde die Sicherheit und Eignung des Systems für eine vorgesehene Anwendung bestätigt. Zu Beginn des Gutachtens sind eine Beschreibung des Begutachtungsgegenstands, des Auftraggebers, der Aufgabenstellung sowie des Ablaufs der Begutachtung einschließlich durchgeführter Audits sowie die Anerkennung des Gutachters darzustellen. Ein tabellarischer Überblick über die während der Produktentwicklung und bei der Erstellung der zugehörigen Dokumentation verwendeten Normen und weiterer Dokumente gibt einen umfassenden Überblick über den genutzten Stand der Technik. In der Dokumentation ist auf relevante Regelwerke und Normen sowie auf genutzte interne und externe Dokumente genau wie auf vorangegangene Sicherheitsnachweise zu verweisen. Die Referenzen erleichtern die Abgrenzung des Begutachtungsgegenstands, wobei die Angabe der Versionsnummer und des Erstelldatums zur Nachverfolgung dienen. Eine mögliche Struktur des Gutachtens wird in Tabelle 8-1 vorgeschlagen.

Tabelle 8-1: Struktur des Gutachtens für sicherheitsrelevante Systeme im Schienenverkehr

Kapitel	Name	Notwendiger Inhalt
1	Einführung	Zweck, Ziel, Beteiligte, Methodik, Betrachtetes Produkt, verbundene Dokumente, Änderungshistorie, Abkürzungen
2	Hintergrund der Begutachtung	Herausforderungen, Gründe, zertifizierungsrelevante Dokumente, angewandte normative und spezifische Dokumente, zu begutachtende Dokumente
3	Begutachtungsgegenstand	Dokumentation der sicheren Entwicklung, Ansatz und technisches Konzept der Entwicklung, beabsichtigte Nutzung der Entwicklung, zu begutachtende Dokumente
4	Nachweis der Begutachtung	Begutachtungsmethode, Qualitäts- und Sicherheitsmanagement des Herstellers, Nachweis der Sicherheit, Komponenten des zu zertifizierenden Systems, Systemspezifikationen und Systemarchitektur, Schnittstellen, Einhaltung der System- und Sicherheitsanforderungen, Hardware- und Softwarefunktionalität, Umgang mit neuen Gefährdungen, Beziehung zu anderen Sicherheitsnachweisen, Ansatz der Begutachtungsmethode, Ansatz des Sicherheitsnachweises des Herstellers
5	Zusammenfassung	Analyse, ob quantitative und qualitative Sicherheitsanforderungen erfüllt werden

Die Tiefe der Begutachtung richtet sich nach der Komplexität des Systems und dem angestrebten Sicherheitslevel. Das Gutachten ist so anzufertigen, dass eine zielstrebige Durchsicht und somit Zertifizierung durch die Sicherheitsbehörde möglich ist. Dafür werden zunächst neue mit vorherigen Komponenten verglichen. Bezüglich des zu zertifizierenden Produkts sind technische Beschreibungen sowie relevante Dokumente, Gesetze, Anforderungen und Referenzdokumente von Bedeutung. Zudem werden die Funktionsliste und sicherheitsbezogene Anwendungen betrachtet. Dabei wird geprüft, ob Risiko- und Sicherheitsanforderungen auf das Produkt und das Anwendungsgebiet abgestimmt sind und eingehalten werden. Falls dies nicht der Fall ist, kann eine Stellungnahme abgegeben werden, wie eine Zertifizierung möglich ist.

Wenn das Gutachten andere Gutachten für (Teil-)Systeme einschließen soll, sind diese zu referenzieren. Dies gilt ebenso für durchgeführte Tests, bspw. im Labor oder auf Teststrecken. Auch die Ausschreibung ist von Relevanz, da dort die Aufgaben des Gutachters beschrieben sind. Die Referenzen und unterstützenden Dokumente sind eine entscheidende Grundlage für die Begutachtung, genau wie genutzte unterstützende Dokumente. Damit wird eindeutig beschrieben, auf welchem Dokumentenstand die Begutachtung aufbaut. Dies beinhaltet in Beziehung stehende Sicherheitsnachweise von Subsystemen oder anderen in Beziehung stehenden Systemen.

Die Begutachtung des Sicherheitsnachweises schließt mit einer Zusammenfassung ab. Dort wird die Begutachtung, der Begutachtungsgegenstand und somit auch das fokussierte Fahrzeug/ System reflektiert. Abschließend wird festgestellt, ob die quantitativen und qualitativen Sicherheitsanforderungen erfüllt werden und ob eine Zertifizierung möglich ist und ob diese empfohlen wird. Zudem ist das Ergebnis der Begutachtung darzustellen und die gewählte Nachweismethode zu begründen.

8.5 Abweichungen gegenüber Sicherheitsanforderungen

Der Gutachter überprüft die Einhaltung der normativen Anforderungen, die erfüllt oder mit kleinen bzw. großen formalen oder inhaltlichen Mängeln nicht erfüllt sein können. Dabei erkennt er möglicherweise Teile des Systems, deren Ausführung verbesserungswürdig ist. Im Gutachten müssen Hinweise gegeben werden, wie mit den Abweichungen im Begutachtungsgegenstand gegenüber den normativen Anforderungen umzugehen ist. Diese Regeln können als „sicherheitsrelevante Anwendungsvorschriften“ [VV BAU-STE 4.6 2014] bezeichnet werden. Weiterhin können vom Gutachter Auflagen aufgestellt werden oder eine Befristung der Zertifizierung vorgeschlagen werden, was einer erweiterten Betriebserprobung entspricht. Die Einteilung erfolgt entsprechend der Schwere der normativen Abweichung und der notwendigen Reaktionen. Große inhaltliche Mängel werden als schwerwiegend klassifiziert, kleine inhaltliche Mängel als bedeutend und zusätzlich als unbedeutend, um eine feine Gliederung mit passender Reaktion zu ermöglichen. Formale Mängel werden als Hinweise beschrieben. Zusätzlich wurde die Klassifikation einer Frage eingeführt. Die Einteilung ist in Tabelle 8-2 dargestellt.

Tabelle 8-2: Einteilung der Abweichungen von Anforderungen im Sicherheitsnachweis

Klassifikation	Reaktion	Beschreibung
Schwerwiegend	Bedingung	Muss vor Inbetriebnahme erfüllt sein
Bedeutend	Auflage	Kein Einfluss auf den Entwurfs- oder Entwicklungsprozess, Aufrechterhaltung der Betriebsgenehmigung hängt davon ab Begutachtung kann nicht vor Abschluss beendet werden
Unbedeutend	Empfehlung	Abweichung in der Dokumentation, die keine neue Revision des Dokuments erfordert Von Umsetzungen ist langfristige Aufrechterhaltung der Betriebsgenehmigung abhängig
Formal	Hinweis	Formale Abweichung, die keine neue Revision des Dokuments erfordert
Frage	Antwort	Eine Erläuterung bezüglich eines Gegenstands oder Aspekts ist notwendig. Die zugehörige Antwort kann in die Begutachtung einfließen

Eine schwere Abweichung ist eine sicherheitsrelevante Abweichung im Entwurfs- oder Entwicklungsprozess, welche Änderungen des Entwurfs oder der Prozesse notwendig macht. Hersteller und Betreiber müssen direkt über derartige Abweichungen informiert werden. Vor Mängelbeseitigung kann kein positives Gutachten ausgestellt werden.

Eine Auflage ist eine Reaktion auf eine bedeutende Abweichung und kann bspw. eine notwendige Schulung von Triebfahrzeugführer oder eine Änderung/ Ergänzung von Handbüchern/ Bedienungsanleitungen sein, die während des Betriebes durchzuführen ist. Wenn sich eine Komponente oder System im Prozess der Entwicklung befindet oder die endgültige Zertifizierung noch nicht erfolgt ist, sich das entsprechende Fahrzeug jedoch bereits im betrieblichen Einsatz befindet, kann eine Auflage sein, dass sich die Komponente auf dem Zug befinden darf, jedoch abgeschaltet sein muss.

Empfehlungen und Hinweise sind Reaktionen auf unbedeutende und formale Abweichungen und sind nützlich, um den Betriebsablauf effizienter zu gestalten oder um die Dokumentation verständlicher aufzubauen und darzustellen. Fragen und Anmerkungen ergänzen die Begutachtung.

8.6 Zulassung des betrachteten Systems

Das Sicherheitsgutachten wird nach Abschluss mit dem Ziel der Zulassung des betrachteten Systems bei der Sicherheitsbehörde eingereicht. Um diesen Schritt durchführen zu können, bestätigt der Gutachter im Gutachten, dass das System entsprechend des Stands der Technik entwickelt wurde und diese Entwicklung im Begutachtungsgegenstand basierend auf dem in Kapitel 3 dargestellten normativen Rahmes konsistent dokumentiert wurde. Zudem wird bestätigt, dass keine sicherheitsrelevanten Abweichungen von den Sicherheitsanforderungen existieren und somit ein sicherer Betrieb des Systems mit keinen oder wenigen Einschränkungen möglich ist.

In TEIV 2004] sind Fristen für die Antwort der Sicherheitsbehörden gesetzt, diese ist innerhalb von vier Monaten vorgeschrieben. Die NSA kann bei nicht Vorliegen grundlegender Anforderungen wie bspw. unzureichender Instandhaltung, Konstruktionsfehlern oder die Funktion einschränkende Defekte entsprechende Maßnahmen ergreifen, die bis zu einem Zurückziehen der Inbetriebnahmegenehmigung reichen können.

9 Zusammenfassung und Ausblick

In dieser Arbeit wurde aufbauend auf den Grundlagen der satellitenbasierten Ortung und des Schienenverkehrs eine generische Methode zur Nachweisführung und zur Zertifizierung einer bordautonomen satellitenbasierten Ortungseinheit für den Schienenverkehr unter Nutzung externer Komponenten eingeführt und angewandt. In diesem abschließenden Kapitel werden in Abschnitt 9.1 die Ergebnisse dieser Arbeit zusammengefasst und in Abschnitt 9.2 ein Ausblick auf weiterführende und vertiefende Forschungsaktivitäten gegeben.

9.1 Zusammenfassung und kritische Diskussion der Ergebnisse

Die sichere Implementierung der satellitenbasierten fahrzeugseitigen Ortung wurde bereits in einer Vielzahl vorangegangener Projekte bearbeitet, woraus verschiedene Prototypen entstanden. Diese zeigten, dass eine satellitenbasierte, sichere Ortung im Schienenverkehr generell möglich ist und einen Beitrag zu einem effizienteren Betrieb im Schienenverkehr liefern kann. In den vergangenen Projekten wurde jedoch nicht die Zertifizierung selbst untersucht. Der dargestellte Entwicklungsprozess ist somit ein bedeutender Fortschritt dieser Arbeit gegenüber dem Stand der Technik.

Die Ergebnisse dieser Arbeit wurden mit Vorgehensweisen erreicht, die auch über diese Arbeit hinaus genutzt werden können. So wurde eine Methodik zur Strukturierung von Anwendungen im Verkehrsbereich erstellt und die Sicherheitsnachweisführung generisch betrachtet. Aufbauend auf einer terminologischen Strukturierung wurde die Systemarchitektur der zu entwickelnden Ortungseinheit erstellt. Für die Funktionen der Ortungseinheit werden im Wesentlichen die aus der Strukturierung der Anwendungen von GNSS resultierenden Eigenschaften genutzt. In diese Betrachtung floss außerdem die strukturierte Darstellung der relevanten Normen ein.

In dieser Arbeit konnte von den in Abschnitt 1.3 gestellten Zielen die Erstellung eines sicherheitsgerichteten Entwicklungsprozesses, die konsistente Darstellung der Systemarchitektur und der Nachweis der sicheren Funktionalität erreicht werden. Die erzielten Ergebnisse bilden eine wichtige Grundlage für die mögliche Einführung der satellitenbasierten fahrzeugseitigen Ortung mit SIL 3 auf Nebenstrecken, die keinen Aktivitäten des Fahrers bedarf. Durch den Entfall teurer streckenseitiger Einrichtungen wird eine Vielzahl von Vorteilen ermöglicht, wodurch die Wettbewerbsfähigkeit des Schienenverkehrs gestärkt werden kann. Die resultierenden Vorteile lassen sich in die Kategorien betrieblich, Sicherheit, Instandhaltung, wirtschaftlich und sozial untergliedern und sind in Tabelle 9-1 zusammengefasst.

Tabelle 9-1: Vorteile der Nutzung der satellitenbasierten Ortung im Schienenverkehr

Betriebliche Vorteile	Vorteile für Instandhaltung	Sicherheitsvorteile	Wirtschaftliche Vorteile	Soziale Vorteile
Kontinuierliche Zugortung	Geringere Schäden durch Vandalismus und bspw. Witterung	Erhöhung der Sicherheit	Marktuntersuchungen	Verkürzte Schließzeit von Bahnübergängen
Höhere Flexibilität in der Disposition	Geringerer Instandhaltungsaufwand	Geringeres Risiko menschlicher Fehler	Zielkostenrechnung für Umsetzungsstrategie	Exakter Halt der Züge an Bahnsteigen
Erhöhte Streckenkapazität	Exakte Ortung von zu reparierenden Streckenabschnitten		Kosteneffizienter Betrieb	Verbesserte Information der Fahrgäste
Kompatible Ortung als Basis für Interoperabilität			Umweltfreundliches Fahren durch präzises Beschleunigen und Bremsen	Reduzierung der Reisezeit
				Verbesserte Zuverlässigkeit des Betriebs

9.2 Ausblick

Gewisse Fernziele des Schienenverkehrs, wie bspw. das fahrerlose Fahren, sind durch eine Kombination der in der Anwendung des Funktionsaspekts dargestellten Subfunktionen der sicheren satellitenbasierten Ortung zu realisieren. Die damit verbundene Automatisierung des Schienenverkehrs würde noch viele weitere Vorteile mit sich bringen, bspw. die Reduzierung der Verantwortung des Betriebspersonals und vielfältige Kosteneinsparungen bspw. der Instandhaltungs- oder Betriebskosten, wofür jedoch hohe Anfangsinvestitionen zu tätigen sind.

Die europaweite Zertifizierung ohne nationale Besonderheiten bedarf möglicherweise über diese Arbeit hinausgehender administrativer Maßnahmen. Sie wäre jedoch hilfreich für die grenzüberschreitende, interoperable Durchführung des Schienenverkehrs. Somit wäre es wünschenswert, wenn – wie für 2016 geplant – eine europäische Behörde eine allgemein gültige Zertifizierung ausstellen könnte. Mit der 2004 gegründeten ERA sind die Voraussetzungen dafür geschaffen, jedoch liegen die entsprechenden Kompetenzen nach derzeitiger Rechtslage bei nationalen Behörden. Für eine allgemein gültige Zertifizierung in Europa wäre zunächst eine europaweite Harmonisierung der Regeln und Betriebsverfahren notwendig.

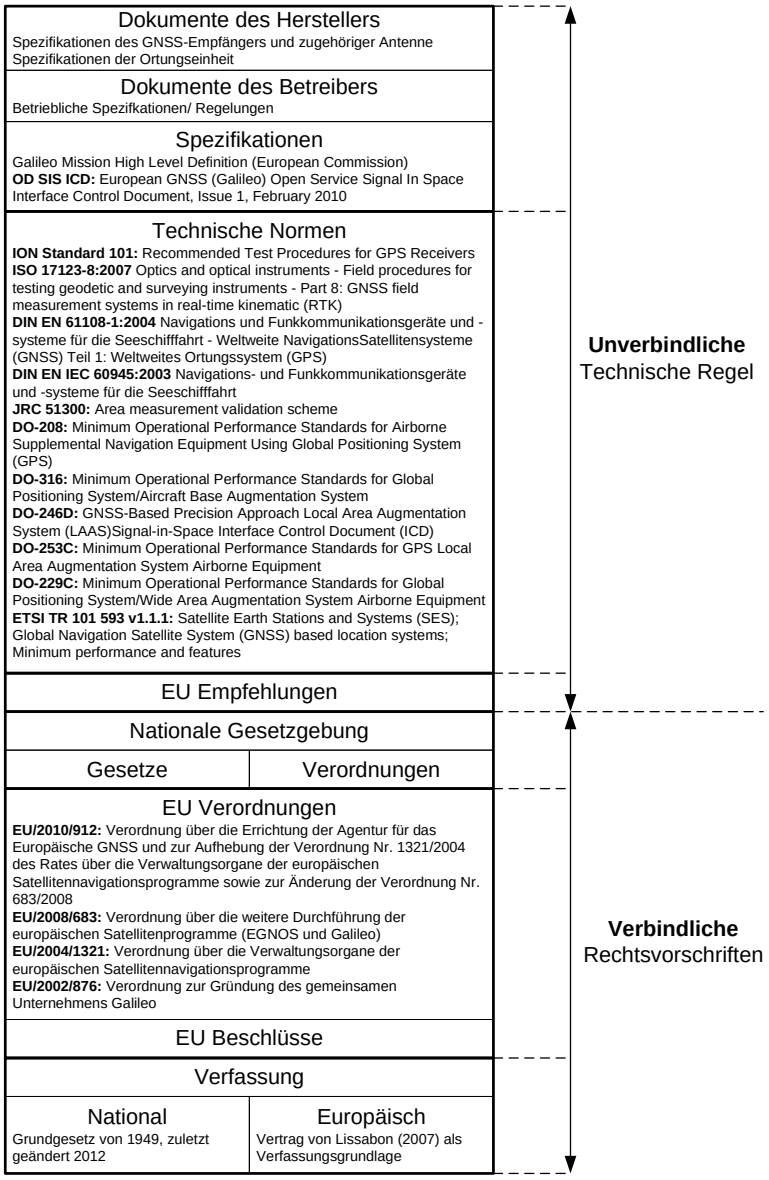
Anhang 1: Projekte zur satellitenbasierten Ortung im Schienenverkehr

Projekt	Dauer	Erfolg	Nicht erreicht
APOLO	1999 – 2001	Erstellung von Spezifikationen, Prototypstudie	Anwendung der Projektergebnisse im Regelbetrieb, Sicherheitsnachweis
GADEROS	2001 – 2004	Nebenstrecken, Kompatibilität mit ERTMS	Anwendung der Projektergebnisse im Regelbetrieb, Sicherheitsnachweis
LOCOPROL	2001 – 2004	Nebenstrecken, Kompatibilität mit ERTMS, GPS Ortungsalgorithmen in Frankreich	Anwendung der Projektergebnisse im Regelbetrieb, Sicherheitsnachweis
INTEGRAIL	2001 – 2004	Multisensorortung	Gleisselektive Ortung bei parallelen Gleisen
ECORAIL	2001 – 2005	Sicherung von Bahnübergängen mit EGNOS	Weitere Anwendungen
GEORAIL	2004 – 2006	Europäisches Referenzsystem für Karten in Schienenverkehrs-anwendungen auf Basis von EDTR89	Anwendung von GNSS im Schienenverkehr
RUNE	2004 – 2006	Virtuelle Balise, sicherheitsrelevante Anwendung, Nutzung von EGNOS	Anwendung der Projektergebnisse im Regelbetrieb, Sicherheitsnachweis
LOCOLOC	2002 – 2004	Nebenstrecken, Kompatibilität mit ERTMS, GPS Ortungsalgorithmen in Belgien	Anwendung der Projektergebnisse im Regelbetrieb, Sicherheitsnachweis
GIRASOLE	nicht bekannt	Multimodaler Galileo SoL Empfänger	Sicherheitsnachweis für Anwendungen im Regelbetrieb
GRAIL 1	2005 – 2007	Empfänger für den Schienenverkehr auf Basis des multimodalen GIRASOLE Empfängers	Sicherheitsnachweis für Anwendungen im Regelbetrieb
TR@IN-MD	2006 – 2009	Verfolgung von gefährlichen Gütern	Sicherheitsnachweis, weitere Anwendungen
LOCASYS	2006 – 2009	Verlässlichkeit von GNSS über einen längeren Zeitraum	Sicherheitsnachweis; Anwendungen im Regelbetrieb
GRAIL2	2010 – 2013	GNSS Architektur für Schienenverkehr	Finalisierung der fahrzeugseitigen Ausrüstung
GaLoROI	2012 – 2014	Zertifizierbare satellitenbasierte Ortungseinheit	Serienfertigung
SATLOC	2012 – 2014	Demonstration eines satellitenbasierten Zugsicherungssystems	Sicherheitsnachweis
EATS	2012 – 2016	Modellierung des ETCS Systemverhaltens und Migration	Anwendung der Projektergebnisse im Regelbetrieb
SAGITER	2013 – 2015	Gemeinsame Standards für satellitenbasierte Ortungssysteme	Fertigstellung von Standards

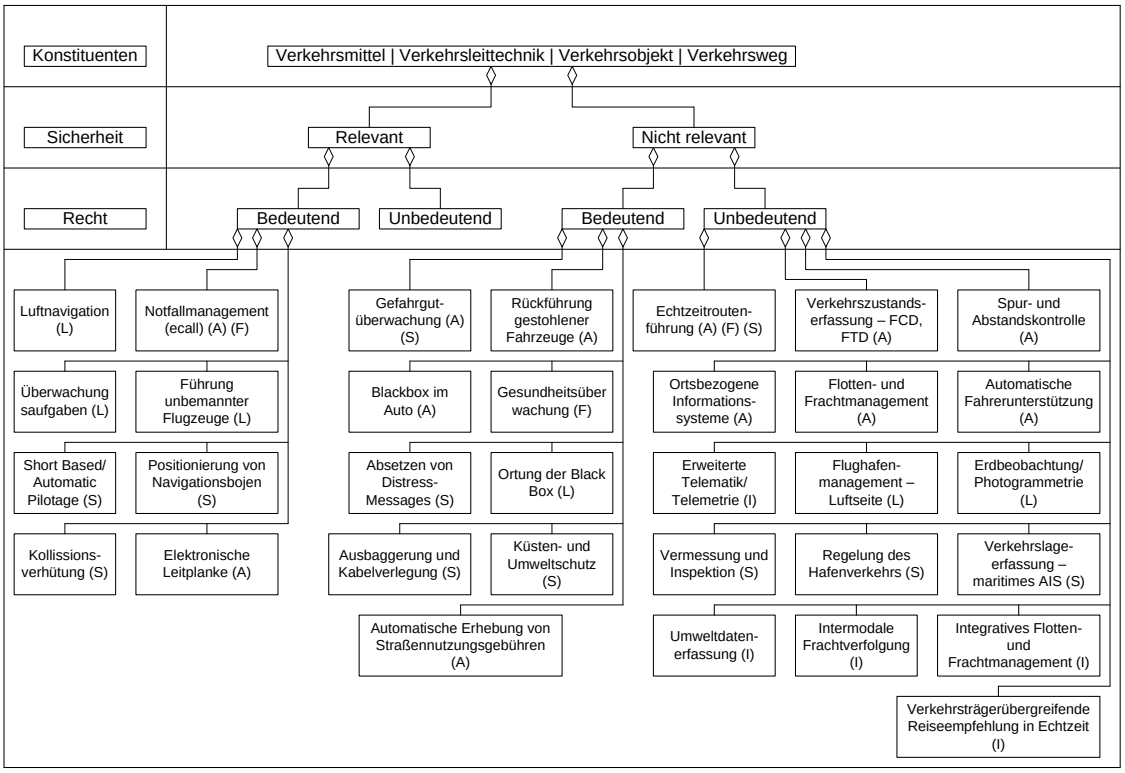
Anhang 2: Bekannte ETCS Ausrüstung in Europa

Streckentyp	Land	Strecke	ETCS Level	Strecken-länge [km]	Anzahl Balisen	Balisen pro km und Gleis	Termin
Bestand	AT	Wels – Passau	1	80			
Bestand	AT	Wien – Hohenau	2	87			
Bestand	AT	Attnang – Salzburg	1	75			
Bestand	AT	Wien – St. Pölten	2	55			
Bestand	AT	Wien – Nickelsdorf	1	70			
Bestand	AT	Kufstein – Umfahrung Innsbruck – Brenner	2	108	2000	7	
Neubau	AT	Kundl – Baumkirchen	2	40			
Neubau	AT	Wien – St. Pölten	2	60	1390	12	
Neubau	CH	Mattstetten – Rothrist	2	45			
Bestand	CH	Solothurn – Wanzwill	2	9			
Neubau	CH	Lötschberg-Basistunnel	2	34	230	3	
Bestand	LU	Gesamtnetz	1	275			
Bestand	SI	Sežana/ Koper – Ljubljana – Hodos	1	350			
Bestand	CH	Brunnen (exkl.) – Altdorf – Rynächt	2	18			
Bestand	CH	Pollegio Nord – Castione Nord	2	20			
Bestand	CH	Pully – Villeneuve	2	28			
Neubau	DE	Erfurt – Leipzig/Halle	2	123	2000	3	
Neubau	DE	Nürnberg – Erfurt	2	189			2017
Neubau	CH	Gotthard-Basistunnel	2	57	928	8	2016
Bestand	CH	Sion – Sierre	2	16			2016
Neubau	AT	St.Pölten – Loosdorf	2	25			2017
Bestand	CH	Giubiasco – S.Antonino	2	2			2018
Neubau	CH	Ceneri-Basistunnel	2	15			2019
Bestand	CH	Roche VD – Vernayaz	2	28			2018-2020
Bestand	CH	Visp – Simplon	2	20			2020
Neubau	AT	Pottendorfer Linie	2	50			2023
Neubau	AT	Graz – Klagenfurt (Koralmbahn)	2	130			2023
Neubau	AT	Semmeringbasistunnel	2	28			2024
Neubau	AT	Brennerbasistunnel	2	55			2025
Neubau	AT	Linz – Wels	2	25			2025

Anhang 3: Normativer Rahmen der satellitenbasierten Ortung



Anhang 4: Strukturierung der Funktionen in anderen Verkehrsdomänen



Anhang 5: Anforderungen an Komponenten in Schienenfahrzeugen

Umweltbedingung	Anforderung	Quelle
Höhenlage	Versch. Klassen, z.B. A1: bis 1400m, AX: mehr als 1400m	DIN EN 50125-1 DIN EN 50125-3
Druckimpulse	Druckänderung in Tunneleinfahrten $\Delta P = \pm 5$ kPa bzw. $\Delta P/\Delta t = 0{,}5$ bis 1 kPa/s	DIN EN 50125-3
Temperatur innerhalb des Fahrzeug	Versch. Klassen, z.B. T1: -25°C bis +50°C, TX: -40°C bis +60°C	DIN EN 50125-1
	Versch. Klassen, z.B. T1: -25°C bis +70°C, TX:-55°C bis +70°C Zusätzlich sind schnelle Temperaturänderungen zu berücksichtigen	DIN EN 50125-3
	Versch. Klassen, z.B. für Innere Schranktemperatur T1: -25°C bis +55°C, TX: -40°C bis +70°C	DIN EN 50155
Temperatur außerhalb des Fahrzeugs	Versch. Klassen, z.B. T1: -25°C bis +40°C, TX: -40°C bis +50°C	DIN EN 50125-1 DIN EN 50155
	Versch. Klassen, z.B. T1: -25°C bis +40°C, TX: -55°C bis +40°C	DIN EN 50125-3
Luftfeuchte	Jahresmittelwert: ≤75 %, kurzfristig höher, es wird auf die Problematik in Tunneln und von gefrierenden Kondenswasser hingewiesen	DIN EN 50125-1 DIN EN 50155
	Versch. Klassen, z.B. im Freien T1: 15 % bis 100 %, T2: 20 % bis 100 %	DIN EN 50125-3
Regen	Regenmenge: 6 mm/min, zu betrachten in Verbindung mit Wind und Fahrzeugbewegungen	EN 60721-3-5
	Versch. Klassen, T1 und T2 bis 6 mm/min, TX bis 15 mm/min	DIN EN 50125-3
Schnee	Versch. Klassen, z.B. S1: 0 mm bis 250 mm, S3 400 mm bis 800 mm, auch müssen Schneeansammlungen und Schmelzen berücksichtigt werden	DIN EN 50125-1
Hagel	Hagelkörner bis 15 mm, größere im Einzelfall	DIN EN 50125-1 DIN EN 50125-3
Eis	Eisbildung und herabfallendes Eis muss berücksichtigt werden	DIN EN 50125-1
	Funktion der Betriebsmittel muss in Produktnorm oder durch Kunden spezifiziert werden	DIN EN 50125-3
Sonnenstrahlung	Versch. Klassen, z.B. R2: 1120 W/m², Thermische Auswirkung und UV-Strahlung muss berücksichtigt werden, max. Sonnenscheindauer von 8h darf angenommen werden	DIN EN 50125-1 DIN EN 50125-3
Blitzschlag	Berücksichtigung von Einflüssen durch Blitzschlag auf Fahrzeug	DIN EN 50124-2
Tiere im Gleis	Gewicht 200 bis 800 kg	DIN EN 50125-1
Wind	Unterscheidung natürlicher Wind (max 35 m/s) und vorbeifahrende Züge (sehr komplex)	DIN EN 50125-3
Brandschutz	Verweis auf Produktnormen	DIN EN 50125-3
Schwingungen und Stöße	Betriebsmittel sollen dort eingebaut werden, wo Schwingungen minimal sind, versch. Grenzwerte [m/s²]	DIN EN 50125-3
	Während des Betriebs darf es nicht zur Verschlechterung der Eigenschaften	DIN EN 50155
Elektromagnetische Verträglichkeit	Verweis auf Prüfbedingungen EN 50121-4 sowie EN 50121-3-2	DIN EN 50125-3-1
	Einrichtungen müssen gegen abgestrahlte Störungen resistent sein und darf keine Funkfrequenzstörungen oberhalb der in EN 50121-3-2 festgelegten Grenzwerte aussenden	DIN EN 50155
Atmosphärische Schadstoffe	Ölnebel, Salzsprühnebel, leitfähiger Staub, Schwefeldioxid	DIN EN 50155

Literaturverzeichnis

[AEUV 2010] Europäische Union: **Vertrag über die Arbeitsweise der Europäischen Union** AEUV, 2010.

[Alcouffe/Barbu 2001] Alcouffe, F.; Barbu, G.: **Apolo** Advanced Position Locator System. Final Report, 2001.

[Amt für Veröffentlichungen 2014] Amt für Veröffentlichungen: **EUR-Lex**. <http://eur-lex.europa.eu>.

[Ansaldo STS 2014] Ansaldo STS: **3INSAT** Trin Integrated Safety Satellite System. <http://artes-apps.esa.int/projects/3insat>, Rev. 2014-02-15.

[ARA 2009] Australian Railway Association (ARA): **Australian Digital Train Control System,** Canberra, 2009.

[ARTC 2015] Australian Rail Track Corporation (ARTC): **Advanced Train Management System** Schedule. <https://atms.artc.com.au/schedule/>.

[Balliet 2011] Balliet, J.B.: **Bridging the European and U.S. Rail Safety Assurance Gap** The Feasibility of Cross Acceptance. Hrsg: AREMA: Proceedings Of The 2011 Annual Conference, Minneapolis, MN, 2011.

[Barbu 2012] Barbu, G.: **SATLOC** Project summary. <http://satloc.uic.org>.

[Bauer 2011] Bauer, M.: **Vermessung und Ortung mit Satelliten** Globale Navigationssatellitensysteme (GNSS) und andere satellitengestützte Navigationssysteme, 6., Wichmann, Berlin [u.a.], 2011.

[Becker/Manz 2016] Becker, U.; Manz, H.: **Satellitenbasierte Ortung in der Zugsicherung** GaLoROI, in: Deine Bahn, 44 (2016) 2, S. 48–52.

[Bepperling 2008] Bepperling, S.-L.: **Validierung eines semi-quantitativen Ansatzes zur Risikobeurteilung in der Eisenbahntechnik**. TU Braunschweig, Dissertation, 2008.

[Berioli 2013] Berioli, M.: **3InSat**. <http://www.dlr.de/kn/en/desktopdefault.aspx/tabid-2081/6933_read-37809/>.

[Beyer/Fußy 2014] Beyer, S.; Fußy, M.: **Herausforderungen bei der Realisierung des DB-Projektes VDE 8**. Hrsg: DVV Media Group: Int. Signal+Draht Kongress, Fulda, 2014.

[Bikker/Schroeder 2002] Bikker, G.; Schroeder, M.: **Methodische Anforderungsanalyse und automatisierter Entwurf sicherheitsrelevanter Eisenbahnleitsysteme mit kooperierenden Werkzeugen**. TU Braunschweig, Dissertation. 529, VDI-Verl., Düsseldorf, 2002.

[Blaauboer et al. 2013] Blaauboer, M.; Mennen, W.; van der Werff, M.: **Reducing Life Cycle Costs of main line interlockings**, in: Signal+Draht, 105 (2013) 11, S. 30–33.

[BMVBS 2011] BMVBS: **Handbuch Eisenbahnfahrzeuge** Leitfaden für Herstellung und Zulassung, Berlin, 2011.

[BMVBS 2013] BMVBS: **Memorandum of Understanding** Über die Neugestaltung von Zulassungsverfahren für Eisenbahnfahrzeuge, Bundesministerium für Verkehr, Bau und Stadtentwicklung, Berlin, 2013.

[Boileau 2014] Boileau, L.: **Bridging the European and North American Rail Safety Assurance Gaps** Examples of Typical Cases of Cross Acceptance in Both Directions. Hrsg: AREMA: Proceedings Of The 2014 Annual Conference & Exposition, Chicago, IL, 2014.

[Bornschlegl 2014] Bornschlegl, S.: **In die richtige Bahn gelenkt** Robuste Rechnerformate für Züge. Rugged Computing, in: Elektronik, 63 (2014) 25, S. 30–34.

[Braband 2005] Braband, J.: **Risikoanalysen in der Eisenbahn-Automatisierung**, 1, Eurailpress, Hamburg, 2005.

[Braband 2006] Braband, J.: **Die CENELEC-Normen zur funktionalen Sicherheit** The CENELEC standards regarding functional safety, Eurailpress, Hamburg, 2006.

[CEN 2010] CEN: **Supporting Material - Guidance documents**. <http://www.cen.eu/BOSS/SUPPORTING/Pages/default.aspx>.

[CENELEC 2013] CENELEC: **What we do**. <http://www.cenelec.eu/aboutcenelec/contactus/contact_entry.htm>.

[China National Space Administration 2016] China National Space Administration: **BeiDou** Navigation Satellite System. <http://en.beidou.gov.cn/>, Rev. 2014-10-21.

[Connor et al. 2014] Connor, P.; Schmid, F.; Watson, C.: **A Review of Train Protection Systems**. <http://www.railway-technical.com/atpsurvey.shtml>.

[Cramer 2012] Cramer, M.: **Alle Signale auf Grün? Fachgespräche zur Zukunft von ERTMS**, in: Signal, 33 (2012) 3, S. 23.

[Däubler et al. 2002] Däubler, L.; Bikker, G.; Schnieder, E.: **SATNAB - Satellitengestütztes Navigations-Bodenexperiment**, in: Signal+Draht, 94 (2002) 6, S. 12–15.

[DB Ril 436] DB Netze: **Zugleitbetrieb**, 2011. <http://fahrweg.dbnetze.com/file/2360810/data/rw_436.pdf>, Rev. 2011.

[Defence Standard 00-56] UK Ministry of Defence: **Safety Management Requirements for Defence Systems**, Issue 4, UK Defence Standardization, Glasgow, 2007. <www.skybrary.aero/bookshelf/books/344.pdf>, Rev. 2007-06-01.

[Dekker 2006] Dekker, S.: **The field guide to understanding human error**, Ashgate, Aldershot, England, Burlington, VT, 2006.

[DemoOrt 2009] DemoOrt: **Development of a Demonstrator for Localization tasks with safety-responsibility in rail freight traffic - DemoOrt** DemoOrt - Abschlussbericht der Phasen 1 und 2, Braunschweig, 2009.

[DIN EN 15380-1] Deutsches Institut für Normung: **Bahnanwendungen – Kennzeichnungssystematik für Schienenfahrzeuge – Teil 1: Grundlagen**, Beuth Verlag, Berlin, 2006, Rev. 2006.

[DIN EN 15380-2] Deutsches Institut für Normung: **Bahnanwendungen – Kennzeichnungssystematik für Schienenfahrzeuge – Teil 2: Produktgruppen**, Beuth Verlag, Berlin, 2006, Rev. 2006.

[DIN EN 15380-3] Deutsches Institut für Normung: **Bahnanwendungen – Kennzeichnungssystematik für Schienenfahrzeuge – Teil 3: Kennzeichnung von Aufstellungs- und Einbauorten**, Beuth Verlag, Berlin, 2006, Rev. 2006.

[DIN EN 15380-4] Deutsches Institut für Normung: **Bahnanwendungen – Kennzeichnungssystematik für Schienenfahrzeuge – Teil 4: Funktionsgruppen**, Beuth Verlag, Berlin, 2013, Rev. 2013.

[DIN EN 15380-5] Deutsches Institut für Normung: **Bahnanwendungen - Kennzeichnungssystematik für Schienenfahrzeuge - Teil 5: Systemstruktur**, Beuth Verlag, Berlin, 2014, Rev. 2014.

[DIN EN 50121-3-2] Verband der Elektrotechnik, Elektronik und Informationstechnik: **Bahnanwendungen - Elektromagnetische Verträglichkeit - Teil 3-2: Bahnfahrzeuge – Geräte**, Beuth Verlag, Berlin, 2007, Rev. 2007.

[DIN EN 50126] Verband der Elektrotechnik, Elektronik und Informationstechnik: **Bahnanwendungen - Spezifikation und Nachweis der Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit, Sicherheit (RAMS)**, Beuth Verlag, Berlin, 1999, Rev. 1999.

[DIN EN 50128] Verband der Elektrotechnik, Elektronik und Informationstechnik: **Bahnanwendungen - Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme - Software für Eisenbahnsteuerungs- und Überwachungssysteme**, 2012-03, Beuth Verlag, Berlin, 2012, Rev. 2012.

[DIN EN 50129] Verband der Elektrotechnik, Elektronik und Informationstechnik: **Bahnanwendungen - Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme - Sicherheitsrelevante elektronische Systeme für Signaltechnik**, Beuth Verlag, Berlin, 2003, Rev. 2003.

[DIN EN 50155] Verband der Elektrotechnik, Elektronik und Informationstechnik: **Bahnanwendungen - Elektronische Einrichtungen auf Bahnfahrzeugen**, Beuth Verlag, Berlin, 2007, Rev. 2007.

[DIN EN 81346-1] Deutsches Institut für Normung: **Industrielle Systeme, Anlagen und Ausrüstungen und Industrieprodukte – Strukturierungsprinzipien und Referenzkennzeichnung – Teil 1: Allgemeine Regeln**, 2010, Beuth Verlag, Berlin, 2010, Rev. 2010.

[DIN EN 81346-2] Deutsches Institut für Normung: **Industrielle Systeme, Anlagen und Ausrüstungen und Industrieprodukte – Strukturierungsprinzipien und Referenzkennzeichnung – Teil 2: Klassifizierung von Objekten und Kennbuchstaben von Klassen**, Beuth Verlag, Berlin, 2010, Rev. 2010.

[DIN EN IEC 61226] Deutsches Institut für Normung: **Kernkraftwerke - Leittechnische Systeme mit sicherheitstechnischer Bedeutung - Kategorisierung leittechnischer Funktionen**, Beuth Verlag, Berlin, 2009, Rev. 2009.

[DIN EN ISO 12100] Deutsches Institut für Normung: **Sicherheit von Maschinen**, Beuth Verlag, Berlin, 2011, Rev. 2011.

[DIN EN ISO 9000] Deutsches Institut für Normung: **Qualitätsmanagement**, Beuth Verlag, Berlin, 2015, Rev. 2015.

[DIN EN ISO 9001] Internationale Organisation für Normung: **Qualitätsmanagementsysteme – Anforderungen**, Beuth Verlag, Berlin, 2015, Rev. 2015.

[DIN EN ISO/ IEC 17011] Deutsches Institut für Normung: **Konformitätsbewertung - Allgemeine Anforderungen an Akkreditierungsstellen, die Konformitätsbewertungsstellen akkreditieren**, 2005, Beuth Verlag, Berlin, 2005, Rev. 2005.

[DIN EN ISO/ IEC 17065] Deutsches Institut für Normung: **Konformitätsbewertung - Anforderungen an Stellen, die Produkte, Prozesse und Dienstleistungen zertifizieren**, 2012, Beuth Verlag, Berlin, 2012, Rev. 2012.

[DIN ISO 81346-3] Deutsches Institut für Normung: **Industrielle Systeme, Anlagen und Ausrüstungen und Industrieprodukte – Strukturierungsprinzipien und Referenzkennzeichnung – Teil 3: Anwendungsregeln für ein Referenzkennzeichensystem**, Beuth Verlag, Berlin, 2013, Rev. 2013.

[DIW 2014] Deutsches Institut für Wirtschaftsforschung (DIW): **Verkehr in Zahlen** 2013/ 2014, 42, DVV Media Group GmbH, Hamburg, 2014.

[DO 178C] RTCA: **Software Considerations in Airborne Systems and Equipment Certification**, RTCA, Washington D.C., 2011, Rev. 2011.

[DO 208] RTCA: **Minimum Operational Performance Standards for Airborne Supplemental Navigation Equipment Using Global Positioning System (GPS)**, RTCA, Washington D.C., 1991, Rev. 1991.

[DO 229D] RTCA: **Minimum Operational Performance Standards for Global Positioning System/Wide Area Augmentation System Airborne Equipment**, RTCA, Washington D.C., 2006, Rev. 2006.

[DO 253C] RTCA: **Minimum Operational Performance Standards for GPS Local Area Augmentation System Airborne Equipment**, RTCA, Washington D.C., 2008, Rev. 2008.

[DO 254] RTCA: **Design Assurance Guidance for Airborne Electronic Hardware**, RTCA, Washington D.C., 2000, Rev. 2000.

[Dodel/Häupler 2009] Dodel, H.; Häupler, D.: **Satellitennavigation**, 2, Springer Berlin, Berlin, 2009.

[Drewes 2009] Drewes, J.: **Verkehrssicherheit im systemischen Kontext**. TU Braunschweig, Dissertation, 2009.

[EBA 2012] Eisenbahnbundesamt (EBA): **Technischer Sicherheitsplan** Sicherheitsrichtline Fahrzeug. SIRF 400 Anlage 1 TeSiP, Bonn, 2012. <http://www.eba.bund.de/SharedDocs/Publikationen/DE/Fahrzeuge/Fahrzeugtechnik/Funktionale_Sicherheit/31_Anlage_1_SIRF_Tesip_Funktionsliste.xls?__blob=publicationFile&v=1>.

[EBA 2013] EBA: **Liste der stillgelegten (DB-) Strecken** seit 01.01.1994. <http://www.eba.bund.de/SharedDocs/Publikationen/DE/Infrastruktur/Stilllegung/stilllegung_brd.xls?__blob=publicationFile&v=3>, Rev. 2013-07-08.

[EBA 2014] Eisenbahnbundesamt (EBA): **TSI CR LOC PAS 2011 NNTR-Gesamtliste**. <http://www.eba.bund.de/SharedDocs/Publikationen/DE/Fahrzeuge/Inbetriebnahme/VV_IBG/NNTV_NNTR/01_NNTV_NNTR_TSI_LOC_PAS.pdf?__blob=publicationFile&v=3>, Rev. 2014-11-20.

[EBA 2015] Eisenbahnbundesamt (EBA): **Verfahren für die Inbetriebnahmegenehmigung von Eisenbahnfahrzeugen nach dem Memorandum of Understanding** Informationen für den Antragsteller, Bonn, 2015.

[EBO 2012] Bundesminister für Verkehr: **Eisenbahn-Bau- und Betriebsordnung** EBO, 1967.

[EC 2006] Europäische Kommission (EC): **ERTMS - für einen flüssigen und sicheren Eisenbahnverkehr** Ein europäisches wirtschaftliches Großvorhaben, Amt für Amtliche Veröff. der Europ. Gemeinschaften, Luxemburg, 2006.

[EC 2012] Europäische Kommission (EC): **EU transport in figures**, Amt für Veröffentlichungen, Luxemburg, 2012.

[EC 2013a] Europäische Kommission (EC): **Length of TEN-T roads per country and link type**. <http://ec.europa.eu/transport/themes/infrastructure/ten-t-policy/transport-mode/doc/road_tab1.pdf>, Rev. 2013-10-16.

[EC 2013b] Europäische Kommission (EC): **Standardisation - Mandates**. <http://ec.europa.eu/enterprise/standards_policy/mandates/database/index.cfm?fuseaction=refSearch.search>.

[EC 2015] Europäische Kommission (EC): **Internal Market, Industry, Entrepreneurship and SMEs** Single Market and Standards. Legislations. <http://ec.europa.eu/enterprise/newapproach/nando/index.cfm?fuseaction=directive.main>, Rev. 2015-03-18.

[EC/ESA 2002] European Commission (EC); European Space Agency (ESA): **Galileo** Mission High Level Definition, 2002.

[Edwards 2000] Edwards, C.J.: **Aircraft operators have built a generic hazard model for use in developing safety cases**, in: ICAO Journal, 55 (2000) 1, S. 12–14,27.

[Eisenbahn-Cert 2015] Eisenbahn-Cert: **Koordinierungsgruppe der Benannten Stellen** NB-Rail. <http://www.eisenbahn-cert.de/DE/Informationen/NB_Rail/nb_rail_node.html>, Rev. 2015-03-18.

[Eisweiler/Steinebach 2014] Eisweiler, B.; Steinebach, P.: **Entwicklung und Umsetzung von Konformitätstests in der Leit- und Sicherungstechnik**, in: Signal+Draht, 106 (2014) 6, S. 10–12.

[Elkins/Carter 1993] Elkins, J.A.; Carter, A.: **Testin and Analysis Techniques for Safety Assessment of Rail Vehicles: The State-of-the-Art**, in: International Journal of Vehicle Mechanics and Mobility, 22 (1993) 3-4, S. 185–208.

[Engelberg 2001] Engelberg, T.: **Geschwindigkeitsmessung von Schienenfahrzeugen mit Wirbelstrom-Sensoren**. Universität Karlsruhe, Dissertation. 896, VDI-Verlag, Düsseldorf, 2001.

[Engelhardt et al. 2011] Engelhardt, T.; Rütters, R.; Katriniok, A.; Abel, D.: **automotiveGATE und railGATE, Testgebiete für Galileo-basierte Fahrzeugführung auf Schiene und Straße**. In: Der 12. Branchentreff der Mess- und Automatisierungstechnik ; Kongress Baden-Baden, 28. und 29. Juni 2011. Hrsg: Adolphs, Peter: Automation 2011. VDI-Verl, Düsseldorf, 2011. (VDI-Berichte, 2143).

[ERA 2014] European Railway Agency (ERA): **Status of TSIs as of April 2014**. <http://www.era.europa.eu/Document-Register/Documents/TSIs-chronology-201404.pdf>.

[ERA-REC-02-2007-SAF 2007] European Railway Agency (ERA): **Recommendation on the 1st set of Common Safety Methods** ERA-REC-02-2007-SAF, 2007.

[Erdmann et al. 1994] Erdmann, L.; Schielke, A.G.; Schnieder, E.: **Referenzmodell zur Strukturierung von Leitsystemen**, in: Automatisierungstechnik, 42 (1994) 5, S. 187–197.

[Ericson 2005] Ericson, C.A.: **Hazard analysis techniques for system safety**, Wiley-Interscience, Hoboken, N.J, 2005.

[ETSI 2012] Europäisches Institut für Telekommunikationsnormen (ETSI): **Satellite Earth Stations and Systems (SES); Global Navigation Satellite System (GNSS) based location systems; Minimum performance and features** ETSI TR 101 593 v1.1.1 (2012-09), Sophia-Antipolis, 2012.

[ETSI 2012a] Europäisches Institut für Telekommunikationsnormen (ETSI): **About ETSI**. <http://www.etsi.org/about>, Rev. 2012.

[EU/2004/49] Europäische Kommission (EC): **Richtlinie über Eisenbahnsicherheit in der Gemeinschaft** EU/2004/49, 2004.

[EU/2004/881] Europäische Kommission (EC): **Verordnung zur Einrichtung einer Europäischen Eisenbahnagentur** EU/2004/881, 2004.

[EU/2008/57] Europäische Kommission (EC): **Richtlinie über die Interoperabilität des Eisenbahnsystems in der Gemeinschaft** EU/2008/57, 2008.

[EU/2009/352] Europäische Kommission (EC): **Verordnung über die Festlegung einer gemeinsamen Sicherheitsmethode für die Evaluierung und Bewertung von Risiken** EU/2009/352, 2009.

[EU/2011/217] Europäische Kommission (EC): **Empfehlung zur Inbetriebnahme von strukturellen Teilsystemen und Fahrzeugen** EU/2011/217, 2011.

[EU/2012/88] Europäische Kommission (EC): **Technische Spezifikation für die Interoperabilität der Teilsysteme „Zugsteuerung, Zugsicherung und Signalgebung" des transeuropäischen Eisenbahnsystems** EU/2012/88, 2012.

[EU/2013/402] Europäische Kommission (EC): **Verordnung über die gemeinsame Sicherheitsmethode für die Evaluierung und Bewertung von Risiken** EU/2013/402, 2013.

[EU/2014/1302] Europäische Kommission (EC): **Verordnung über eine technische Spezifikation für die Interoperabilität des Teilsystems „Fahrzeuge — Lokomotiven und Personenwagen" des Eisenbahnsystems in der Europäischen Union** EU/2014/1302.

[EU/2014/897] Europäische Kommission (EC): **Inbetriebnahme und Nutzung von strukturellen Teilsystemen und Fahrzeugen** EU/2014/897, 2014.

[Federal Space Agency 2016] Federal Space Agency: **Information-Analytical Centre** GLONASS constellation status. <http://glonass-iac.ru/en/GLONASS/>, Rev. 2016-01-25.

[Feltz 2014] Feltz, A.: **ETCS am Drehkreuz Luxemburg** D'Lëtzebuerger Eisebunnsnetz. Hrsg: DVV Media Group: Int. Signal+Draht Kongress, Fulda, 2014.

[Fenner et al. 2003] Fenner, W.; Naumann, P.; Trinckauf, J.: **Bahnsicherungstechnik** Steuern, Sichern und Überwachen von Fahrwegen und Fahrgeschwindigkeiten im Schienenverkehr, 2, Publicis Corporate Publ., Erlangen, 2003.

[Fowler 2005] Fowler, T.: **Aviation Safety Cases** The Safety Case and Safety Argument. <http://www-mip.onera.fr/projets/WakeNet2-Europe/fichiers/pastEvents2005/bretigny-november/Tim_Fowler.pdf>, Rev. 2005-11-29.

[FRA 2010] Federal Railroad Administration (FRA): **Rules, standards, and instructions governing the installation, inspection, maintenance, and repair of signal and train control systems, devices, and appliances - Part 236** FRA, 2010.

[FRA 2014] Federal Railroad Administration (FRA): **About FRA**. <http://www.fra.dot.gov/Page/P0002>.

[Fricke/Piereck 1990] Fricke, H.; Piereck, K.: **Verkehrssicherung**, B.G. Teubner, Stuttgart, 1990.

[GAUSS Basisprojekt 2010] GAUSS Basisprojekt: **Entwicklung des Dienstleistungsangebots zur Zertifizierung von sicherheitskritischen Galileo-Anwendungen sowie Aufbau der technischen Infrastruktur** GAUSS – Towards a unified certification process for safety-critical GNSS applications. Berichte aus dem DLR-Institut für Verkehrssystemtechnik, Braunschweig, 2010.

[Geistler 2007] Geistler, A.: **Bordautonome Ortung von Schienenfahrzeugen mit Wirbelstrom-Sensoren**. Karlsruher Institut für Technologie (KIT), Dissertation. 005, KIT - Scientific Publishing, Karlsruhe, 2007.

[Georail 2008] Georail: **Railway geodesy guidelines for use of absolute coordinates in railway geo-referenced applications** UIC project No I/06/L/019, Paris, 2008.

[Gibbons 2014] Gibbons, G.: **India Certifies GAGAN for En Route and NPA Flight Operations**, in: Inside GNSS (2014).

[Gibbons et al. 2013] Gibbons, G.; Divis, D.A.; Gutierrez, P.: **The GNSS Quartet** Harmonizing GPS, GLONASS, BeiDou and Galileo, in: Inside GNSS, 8 (2013) 1.

[GPS World 2011] GPS World: **EGNOS SOL operational**, in: GPS World (2011), S. 5.

[Gralla 2009] Gralla, C.: **Zur Gestaltung einer ETCS-Migration eines Eisenbahnverkehrsunternehmens**. Dissertation, Braunschweig, 2009.

[Grasso Toro 2015] Grasso Toro, F.: **Development of Intelligent GNSS-based Land Vehicle Localisation Systems**. TU Braunschweig, Dissertation, Braunschweig, 2015.

[Grasso Toro et al. 2012] Grasso Toro, F.; Lu, D.; Manz, H.; Schnieder, E.: **Accuracy evaluation of GNSS for a precise vehicle control**. In: CTS 2012. Hrsg: IFAC: 13th IFAC Symposium on Control in Transportation Systems, 2012.

[Grimm et al. 2005] Grimm, M.; Hartwig, K.; Meyer zu Hörste, M.: **Anforderungen an eine sicherheitsrelevante Ortung im Schienenverkehr**. Hrsg: TU Dresden: 20. Verkehrswissenschaftliche Tage. TU Dresden, Dresden, 2005.

[Groves et al. 2010] Groves, B.; Sanders, P.; de Jong, S.: **Advanced Train Management System** ATMS Proof of Concept - ATMS Program Phase II. ATMS Concept of Operations, Melbourne, 2010.

[GSC 2016] European GNSS Service Centre (GSC): **Constellation Information** Constellation Status. <http://www.gsc-europa.eu/system-status/Constellation-Information>, Rev. 2016-01-11.

[Hänsel 2008] Hänsel, F.: **Zur Formalisierung technischer Normen**. TU Braunschweig, Dissertation. 787, VDI-Verlag, Düsseldorf, 2008.

[Hasberg 2011] Hasberg, C.: **Simultane Lokalisierung und Kartierung spurgeführter Systeme**. Karlsruher Institut für Technologie (KIT), Dissertation. 019, KIT - Scientific Publishing, 2011.

[Hausmann/Enders 2007] Hausmann, A.; Enders, D.H.: **Grundlagen des Bahnbetriebs**, 2., überarb. und erw. Aufl., Bahn-Fachverl., Heidelberg, Mainz, 2007.

[Heinisch/Schweinsberg 2003] Heinisch, R.; Schweinsberg, R.: **Liberalisierung und Harmonisierung der Eisenbahnen in Europa**. 2003, Hestra-Verl., Darmstadt, 2003.

[Heller 2013] Heller, H.: **Einsatz in rauer Umgebung am Beispiel der EN 50155** CompactPCI Serial. <http://www.elektronikpraxis.vogel.de/embedded-computing/articles/425975/>, Rev. 2013-11-21.

[Hemsley 2014] Hemsley, P.: **Fresh probe considers shunting Queensland Rail onto national tracks**. <http://www.governmentnews.com.au/2014/02/fresh-probe-considers-shunting-queensland-rail-onto-national-tracks/>, Rev. 2014-02-27.

[Hensel 2011] Hensel, S.: **Wirbelstromsensorbasierte Lokalisierung von Schienenfahrzeugen in topologischen Karten**. Karlsruher Institut für Technologie (KIT), Dissertation, Karlsruhe, 2011.

[Hernández et al. 2015] Hernández, I.F.; Rodriguez, I.; Tobías, G.; Calle, J.D.; Carbonell, E.; Seco-Granados, G.; Simon, J.; Blasi, R.: **Galileo's Commercial Service** Testing GNSS High Accuracy and Authentication, in: Inside GNSS, 10 (2015) 1, S. 38–48.

[Hinzen 1993] Hinzen, A.: **Der Einfluß des menschlichen Fehlers auf die Sicherheit der Eisenbahn**. RWTH Aachen, Dissertation. 48, Aachen, 1993.

[Hofmann-Wellenhof et al. 2008] Hofmann-Wellenhof, B.; Lichtenegger, H.; Wasle, E.: **GNSS-global navigation satellite systems** GPS, GLONASS, Galileo and more, Springer, Wien, New York, 2008.

[Holzhey 2010] Holzhey, M.: **Ausbaukonzeption für einen leistungsfähigen Schienengüterverkehr in Deutschland** Schienennetz 2025/2030. Förderkennzeichen 363 01 244; UBA-FB 001400, Dessau-Roßlau, 2010.

[ICAO 2004] International Civil Aviation Organisation (ICAO): **Navigation Systems Panel - Amendment 79 to the International Standards and Recommended Practices, Aeronautical Telecommunications (Annex 10 to the Convention on International Civil Aviation)** ICAO, 2004.

[ICAO 2005] International Civil Aviation Organisation (ICAO): **Global Navigation Satellite System (GNSS) Manual** Doc 9849 AN/457, 1, Montreal, 2005.

[IEC 61508] Verband der Elektrotechnik, Elektronik und Informationstechnik: **Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme**, 2010, Beuth Verlag, Berlin, 2010, Rev. 2010.

[Innotrans 2013] Innotrans: **Das vierte Eisenbahnpaket nimmt Fahrt auf** Eisenbahnverbände und europäische Kommission fordern technische Reformen, in: InnoTrans, 17 (2013) 2, S. 1.

[Kaplan/Hegarty 2006] Kaplan, E.D.; Hegarty, C.: **Understanding GPS** Principles and applications, 2nd ed., Artech House, Boston, 2006.

[Kelly/Weaver 2004] Kelly, T.; Weaver, R.: **The Goal Structuring Notation – A Safety Argument Notation**. In: Best Practices, Possible Obstacles, and Future Opportunities. Hrsg: IEEE: Workshop on Assurance Cases, 2004.

[Kiriczi 1996] Kiriczi, S.B.: **Signaltechnisch sichere Fehlergrenzen für die Erfassung der Bewegungszustände von Bahnen**. 583, VDE Verlag, Düsseldorf, 1996.

[Klinge 1998] Klinge, K.-A.: **Konzept eines fahrzeugautarken Ortungsmoduls für den spurgebundenen Verkehr**. TU Braunschweig, Dissertation, Shaker, Aachen, 1998.

[Koppers et al. 2000] Koppers, L.; Heister, H.; Musäus, S.; Plan, O.; Reinhardt, W.: **ALOIS - An Integrated Train Positioning and Information System**. Hrsg: Schnieder, Eckehard, Becker, Uwe: 9 th IFAC Symposium Control in Transportation Systems, 2000.

[Körkemeier 2013] Körkemeier, H.: **Gleisfreimeldung für wirtschaftlichen Bahnbetrieb** Clearguard ACM 200, in: Signal+Draht, 105 (2013) 11, S. 6–9.

[Körkemeier et al. 2013] Körkemeier, H.; Loch, J.; Raschke, B.; Lude, G.: **Gleisfreimeldung für den wirtschaftlichen Bahnbetrieb** Clearguard TCM 100, in: Signal+Draht, 105 (2013) 3, S. 12–16.

[Lackhove 2013] Lackhove, C.: **Methode zur Optimierung der Migration von ETCS**. TU Braunschweig, Dissertation, Braunschweig, 2013.

[Leinhos 1996] Leinhos, D.: **Analyse und Entwurf von Ortungssystemen für den Schienenverkehr mit Strukturierten Methoden**. TU Braunschweig, Dissertation, 1996.

[Leining 2014] Leining, M.: **Herausforderungen bei der Konzeption und Einführung von ETCS in Deutschland am Beispiel der Interoperabilität**. Hrsg: DVV Media Group: Int. Signal+Draht Kongress, Fulda, 2014.

[Leining et al. 2013] Leining, M.; Elsweiler, B.; Stalp, A.: **Neue Typzulassung (NTZ) - Zulassungsprozesse der Zukunft in der Leit- und Sicherungstechnik**, in: Eisenbahntechnische Rundschau, 62 (2013) 1+2.

[Leveson 2011] Leveson, N.: **The Use of Safety Cases in Certification and Regulation**, in: Journal of System Safety, 47 (2011) 6.

[Leveson 2012] Leveson, N.: **Engineering a safer world** Systems thinking applied to safety, MIT Press, Cambridge, Mass, 2012.

[Lu 2014] Lu, D.: **GNSS for Train Localisation Performance Evaluation and Verification**. TU Braunschweig, Dissertation, Braunschweig, 2014.

[Lu et al. 2012] Lu, D.; Wu, D.; Schnieder, E.: **Hazard Analysis for GNSS-based Train Localisation Unit with Model Based Approach According to EGNOS SoL and Railway RAMS**. In: Challenges & Opportunities. Hrsg: Arab Institute of Navigation: 14th IAIN Congress 2012 Seamless Navigation, 2012.

[Maguire 2006] Maguire, R.: **Safety cases and safety reports** Meaning, motivation and management, Ashgate, Aldershot, England, Burlington, 2006.

[Mansfeld 2009] Mansfeld, W.: **Satellitenortung und Navigation** Grundlagen, Wirkungsweise und Anwendung globaler Satellitennavigationssysteme, Morgan Kaufmann, [S.l.], 2009.

[Marais 2002] Marais, J.: **Localisation de mobiles terrestres par satellites** mise en oeuvre d'outils permettant l'analyse de l'influence des conditions de propagation et des effets de masques sur la disponobilité du service offert. Université Lille I, Dissertation, 2002.

[Marais et al. 2008] Marais, J.; Hänsel, F.; Poliak, J.; Becker, U.; Schnieder, E.: **Methods and Tools for the Certification of GALILEO for Railway Applications**. In: WCRR 2008. Hrsg: Korea Railroad Corporation, Korea Rail Network Authority Korea: Proceedings of the 8th World Congress on Railway Research, Seoul/Korea, 2008.

[Marais/Beugin 2012] Marais, J.; Beugin, J.: **Evaluation method of GNSS-based positioning functions for safety applications in operational conditions**. Hrsg: European Road Transport Research Advisory Council, S. 806–815: Procedia - Social and Behavioral Sciences. Elsevier Ltd., Amsterdam, 2012.

[Maschek 2015] Maschek, U.: **Sicherung des Schienenverkehrs** Grundlagen und Planung der Leit- und Sicherungstechnik, 3., überarb. u. erw. Aufl. 2015, Springer Fachmedien Wiesbaden GmbH, Wiesbaden, 2015.

[May 2010] May, J.C.: **Methodische Sicherheitsuntersuchung für einen innovativen Schienenverkehr am Beispiel der fahrzeugautarken Ortung**. TU Braunschweig, Dissertation, 2010.

[McNeff 2012] McNeff, J.: **GPS Receiver Specifications** Compliance and Certification, in: Inside GNSS, 7 (2012) 3, S. 50–56.

[Meyer zu Hörste 2004] Meyer zu Hörste, M.: **Methodische Analyse und generische Modellierung von Eisenbahnleit- und -sicherungssystemen**. TU Braunschweig, Dissertation. 571, VDI-Verl., Düsseldorf, 2004.

[Meyer zu Hörste et al. 2001] Meyer zu Hörste, M.; Lemmer, K.; Bikker, G.; Schnieder, E.: **A general approach for the development and architecture of satellite-based train control systems**. Hrsg: NavSat: Tagungsband zur NavSat, 2001.

[Meyer zu Hörste et al. 2008] Meyer zu Hörste, M.; Lemmer, K.; Urech, A.; Jose, M.: **The GRAIL project: Galileo Localisation for the European Train Control System**. In: CERGAL. Hrsg: Deutsche Gesellschaft für Ortung und Navigation: International Symposium on Certification of GNSS Systems & Services, Braunschweig, 2008.

[Meyer zu Hörste/Lemmer 2005] Meyer zu Hörste, M.; Lemmer, K.: **Requirements for the use of Galileo in Railway Applications**. In: CERGAL. Hrsg: Deutsche Gesellschaft für Ortung und Navigation: International Symposium on Certification of GNSS Systems & Services, Braunschweig, 2005.

[Michler et al. 2013] Michler, O.; Richter, R.; Wolf, B.; Förster, G.; Kolmorgen, V.P.: **Field and Laboratory Evaluation of Satellite-Based Train Location Systems Using a Multi-Channel Radio Frequency Signal Recorder and Generator**. In: WCRR 2013. Hrsg: Australasian Railway Association (ARA): 10th World Congress on Railway Research, Sydney, 2013.

[MIL STD-882E] USA - Department of Defence: **Standard Practice - System Safety**, 2012. <http://www.system-safety.org/Documents/MIL-STD-882E.pdf>, Rev. 2012-05-11.

[Ministerie van Infrastructuur en Milieu 2013] Ministerie van Infrastructuur en Milieu: **Railway map ERTMS** Version 2.0 – State of play regarding research in the Exploratory Phase, Den Haag, 2013.

[Mü 8004] Bundesbahnzentralamt: **Technische Grundsätze für die Zulassung von Sicherungsanlagen**, Eisenbahn-Bundesamt, Büro München, 1980. <http://books.google.de/books?id=0i2yPgAACAAJ>, Rev. 1980.

[Müller 2015] Müller, J.R.: **Die Formalisierte Terminologie der Verlässlichkeit Technischer Systeme**, Springer, Berlin, Heidelberg, 2015.

[NOAA 2014] National Oceanic and Atmospheric Administration (NOAA): **New Civil Signals**. <http://www.gps.gov/systems/gps/modernization/civilsignals/>, Rev. 2014-04-28.

[Nurmi 2015] Nurmi, J.: **GALILEO positioning technology**. volume 182, Springer, Dordrecht, 2015.

[ÖBB Infra 2014] ÖBB Infra: **Streckenausrüstung mit ETCS**. <http://www.oebb.at/infrastruktur/de/_p_3_0_fuer_Kunden_Partner/3_3_Schieneninfrastruktur/3_3_8_ETCS/02_DMS_Dateien/_ETCS_Ausbauplan.jsp>, Rev. 2014-11-24.

[Obrenovic 2009] Obrenovic, M.: **Methodik für die Migration von Systemen der Eisenbahnleit- und -sicherungstechnik am Beispiel der Einführung von ETCS**. TU Braunschweig, Dissertation, Braunschweig, 2009.

[Pachl 2013] Pachl, J.: **Systemtechnik des Schienenverkehrs** Bahnbetrieb planen, steuern und sichern, 7., überarb. u. erw. Aufl. 2014, Springer Vieweg, Wiesbaden, 2013.

[Petrek 2010] Petrek, N.: **Analyse und Strukturierung der Funktionalitäten von Positive Train Control**. TU Braunschweig, Diplomarbeit, Braunschweig, 2010.

[Petri 1962] Petri, C.A.: **Kommunikation mit Automaten**. Universität Bonn, Dissertation, Bonn, 1962.

[Phadrus Systems 2013] Phadrus Systems: **CATS tools for Safety Critical work**. <http://phaedsys.com/principals/riskcats/index.html>, Rev. 2013.

[Pisek 2014] Pisek, M.: **ETCS in Österreich** Herausforderungen und Erfahrungen bei Umsetzung von ETCS bei der ÖBB. Schwerpunkt Betrieb. Hrsg: DVV Media Group: Int. Signal+Draht Kongress, Fulda, 2014.

[Plan 2004] Plan, O.: **GIS-gestützte Verfolgung von Lokomotiven im Werkbahnverkehr**. Universität der Bundeswehr München, Dissertation. 78, Neubiberg, 2004.

[Poliak 2009] Poliak, J.: **Validierung von satellitenbasierten Eisenbahnortungssystemen**. TU Braunschweig, Dissertation, Braunschweig, 2009.

[Prengel/Stadlbauer 2015] Prengel, R.; Stadlbauer, R.: **Implementierung von ERTMS/ ETCS Level 1 auf dem slowenischen Abschnitt des Korridors D**, in: Signal+Draht, 107 (2015) 11, S. 6–10.

[railML 2013] railML: **Die XML-Schnittstelle für Eisenbahnanwendungen**. <http://www.railml.org>.

[Railway Insider 2010] Railway Insider: **Ansaldo STS tests the implementation of ITARUS-ATC (ERTMS) system in Russia**. <http://rinsider.club-feroviar.ro/en/afiseaza_stire.php?id=5557>, Rev. 2010-01-14.

[Reinbold 2007] Reinbold, F.: **Analyse und Vergleich verschiedener Normungsprozesse**. TU Braunschweig, Studienarbeit, Braunschweig, 2007.

[Reinhardt 2011] Reinhardt, W.: **Offentlicher Personennahverkehr** Technik - Rechts- Und Betriebswirtschaftliche Grundlagen, Vieweg + Teubner Verlag, 2011.

[Rösch 2012] Rösch, W.: **Umsetzung des europäischen Regelwerks für Eisenbahn-Fahrzeugsicherheit**, in: Elektrische Bahnen, 110 (2012) 10, S. 563–569.

[Roth 2014] Roth, U.: **Umsetzung von ETCS bei den SBB**. Hrsg: DVV Media Group: Int. Signal+Draht Kongress, Fulda, 2014.

[Rüsch 2012] Rüsch, F.: **Die "Sicherheitsrichtlinie Fahrzeug" - ein Überblick** Fachliches Resümee der durch den Verband der Bahnindustrie in Deutschland durchgeführten Seminare zur Anwendung der SIRF, in: Der Eisenbahningenieur, 63 (2012) 4, S. 14–17.

[Rüthers/Fischer 2010] Rüthers, B.; Fischer, C.: **Rechtstheorie** Begriff, Geltung und Anwendung des Rechts, 5, C H Beck, München, 2010.

[Rumpe 2011] Rumpe, B.: Modellierung mit UML, Springer; Berlin, 2011.

[Sadauskas 2015] Sadauskas, A.: **Australia's train signalling set to go digital**. <http://www.itnews.com.au/news/australias-train-signalling-set-to-go-digital-408467>, Rev. 2015-08-28.

[SAE 1996] Society of Automotive Engineers (SAE): **Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment**. ARP 4761, Rev. 1996.

[SAE 2010] Society of Automotive Engineers (SAE): **Guidelines For Development Of Civil Aircraft and Systems**. ARP 4754, Rev. 2010.

[Schaffarczik 2002] Schaffarczik, K.: **Der Anwendungsmanager, eine intelligente Softwareplattform zur Nutzung von Bordanzeigegeräten**, in: Eisenbahntechnische Rundschau, 51 (2002) 3, S. 141–148.

[Scheppan 2006] Scheppan, M.: **Zugleitbetrieb für einfache betriebliche Verhältnisse**, Eurailpress, Hamburg, 2006.

[Schnieder 1998] Schnieder, E.: **Automatisierung von Sicherheitsfunktionen für den Schienenverkehr**, in: Automatisierungstechnik, 46 (1998) 2, S. 69–77.

[Schnieder 2007] Schnieder, E.: **Verkehrsleittechnik** Automatisierung des Straßen- und Schienenverkehrs; mit 45 Tabellen, Springer, Berlin [u.a.], 2007.

[Schnieder 2009] Schnieder, E.: **Nutzung von Satellitenortungssystemen für Eisenbahnen im rechtlichen Rahmen** Use of satellite based localization for railways in legal context, in: ZEVRail, 133 (2009) 9, S. 351–357.

[Schnieder 2010] Schnieder, L.: **Formalisierte Terminologien technischer Systeme und ihrer Zuverlässigkeit**. TU Braunschweig, Dissertation, 2010.

[Schnieder 2012] Schnieder, E.: **Qualität dynamischer Satellitenortung im Eisenbahnverkehr**, in: Technisches Messen, 79 (2012) 4, S. 210–219.

[Schnieder et al. 2000] Schnieder, E.; Mesch, F.; Engelberg, T.; Puente, L.F.: **Patent - A device and a method for determining the position of a rail-bound vehicle**. Eddy current sensor, B61L 25/02, 2000, Rev. 2000-03-10.

[Schnieder et al. 2009a] Schnieder, E.; Becker, U.; Hänsel, F.; Manz, H.; Poliak, J.; Schröder, J.; Zhou, Y.: **Entwicklung einer Methodik zur Zertifizierung von Ortungseinrichtungen unter sicherheitsrelevanten Aspekten** ZEUS - Projektabschlussbericht, Braunschweig, 2009.

[Schnieder et al. 2009b] Schnieder, L.; Schnieder, E.; Ständer, T.: **Railway Safety and Security - Two Sides of the Same Coin?!** Hrsg: UIC: International Railway Safety Conference 2009, 2009.

[Schnieder et al. 2011] Schnieder, E.; Müller, J.R.; von Buxhoeveden, G.: **Der Sicherheitsnachweis nach CENELEC 50129: Effizientes Erstellen und Kommunizieren**. Hrsg: VDI: TTZ 2011, 2011.

[Schnieder/Barbu 2009] Schnieder, E.; Barbu, G.: **Potenziale satellitenbasierter Ortung für Eisenbahnen** Potential of satellite based localization for railways, in: Eisenbahntechnische Rundschau, 58 (2009) 1-2, S. 38–43.

[Schnieder/Schnieder 2010] Schnieder, E.; Schnieder, L.: **Terminologische Präzisierung des Systembegriffs**, in: atp edition, 52 (2010) 9, S. 46–59.

[Schnieder/Schnieder 2013] Schnieder, E.; Schnieder, L.: **Verkehrssicherheit** Maße und Modelle, Methoden und Maßnahmen für den Straßen- und Schienenverkehr, Springer Vieweg, Berlin, Heidelberg, 2013.

[Schweinsberg 2011] Schweinsberg, R.: **Risikobewertung nach „CSM" – Herausforderung für den Sektor Schiene?** Sicherheitsmethoden, in: Der Eisenbahningenieur, 62 (2011) 6, S. 43–48.

[Sciutto et al. 2010] Sciutto, G.; Bellini, C.; Gloria, A.: **The role of the Notified Bodies in the process of the railway liberalization**. Hrsg: Sciutto, G.: Safety and security in railway engineering. WIT Press, Southampton, 2010.

[Septentrio 2011] Septentrio: **PolaNt+_MC** GPS/ GLONASS/ Galileo L-Band, Löwen, 2011.

[Seybold 2007] Seybold, J.: **GALCERT** Support to the Certification of Galileo. Project of the European GNSS Supervisory Authority (GSA), Paris, 2007.

[Sheridan 2015] Sheridan, K.: **TasRail implements $11m digital train tracking system**. <http://www.abc.net.au/news/2015-01-22/tasrail-implements-digital-tracking-system/6034902>, Rev. 2015-01-22.

[Shin et al. 2008] Shin, K.-H.; Jeong, R.-G.; Joung, E.-J.: **A study on the reliability improvement for applying GNSS to Railroad System**. In: WCRR 2008. Hrsg: Korea Railroad Corporation, Korea Rail Network Authority Korea, S. 136–137: Proceedings of the 8th World Congress on Railway Research, Seoul/Korea, 2008.

[Shirres 2012] Shirres, D.: **Russian railways shoot for Olympic gold**. <http://www.therailengineer.com/2012/08/02/russian-railways-shoot-for-olympic-gold/>, Rev. 2012-08-02.

[Slovak 2006] Slovak, R.: **Methodische Modellierung und Analyse von Sicherungssystemen des Eisenbahnverkehrs**. TU Braunschweig, Dissertation, Braunschweig, 2006.

[Spiegel et al. 2013] Spiegel, D.; Becker, U.; Schnieder, E.: **GNSS-Ortungsgenauigkeit: Eine Methode zur standardisierten Prüfung**. Hrsg: DGON: Positionierung und Navigation für Intelligente Transportsysteme, Berlin, 2013.

[Spiegel et al. 2014] Spiegel, D.; Grasso Toro, F.; Becker, U.: **A Satellite Independent High Dynamic Test Bed and First Measurement Results**. In: ION GNSS 2014. Hrsg: Institute of Navigation: The 27th International Technical Meeting of the Satellite Division, Tampa, FL, USA, 2014.

[Spiegel/Becker 2015] Spiegel, D.; Becker, U.: **Reliable Receiver Quality Assessment by Means of a Record and Playback System**. Hrsg: European Space Agency (ESA): 5th International Colloquium Scientific and Fundamental Aspects of the Galileo Programme, Braunschweig, 2015.

[Stadlmann 2007] Stadlmann, B.: **GPS-gestützter Zugleitbetrieb: Eine kostengünstige Lösung für die Strecken der Linzer Lokalbahn**. Hrsg: Institut für Regional- und Fernverkehrsplanung: FBS-Anwendertreffen Schwerpunkt Infrastruktur, Dresden, 2007.

[Stadlmann et al. 2012] Stadlmann, B.; Kaiser, F.; Maihofer, S.: **Rechnergestütztes Zugleitsystem für die Pinzgauer Lokalbahn**, in: Signal+Draht, 104 (2012) 5, S. 28–33.

[Standard 1474.1] IEEE: **Standard for Communications-Based Train Control (CBTC) Performance and Functional Requirements**, 2004, 2009, Rev. 2009.

[Standard 1483] IEEE: **Standard for Verification of Vital Functions in Processor-Based Systems Used in Rail Transit Control**, 2000, 2007, Rev. 2007.

[Ständer 2010] Ständer, T.: **Eine modellbasierte Methode zur Objektivierung der Risikoanalyse nach ISO 26262**. TU Braunschweig, Dissertation, Braunschweig, 2010.

[Stanley 2011] Stanley, P.: **ETCS for engineers**, 1., Eurailpress, Hamburg, 2011.

[Stein 2012] Stein, C.: **Intelligente Glossare**, in: Fachzeitschrift für Dolmetscher und Übersetzer, 9 (2012) 3, S. 46–50.

[Steindl 2015] Steindl, H.: **Internationaler SIGNAL+DRAHT-Kongress 2014** S+D Kongress 2014, in: Signal+Draht, 107 (2015) 1+2, S. 6–21.

[Strandberg et al. 2013] Strandberg, A.; Laudon, F.; Morin, H.; Karlsson, A.: **ERTMS Leverantörsdag**, 2013.

[Strang 2007] Strang, T.: **Satellitennavigation als Basis innovativer Verkehrsanwendungen**. Hrsg: Deutsches Zentrum für Luft- und Raumfahrt: Chancen innovativer Technologien, Köln, 2007.

[Strang et al. 2008] Strang, T.; Schubert, F.; Thölert, S.; Oberweis, R.; Angermann, M.; Belabbas, B.; Dammann, A.; Jost, T.; Kaiser, S.; Kelter, H.; Khider, M.; Krach, B.; Lehner, A.; Noack, T.; Remi, P.; Rippl, M.; Robertson, P.; Wagner, H.-P.; Weber, C.; Wendlandt, K.: **Lokalisierungsverfahren**, Shaker, Aachen, 2008.

[TEIV 2004] Bundesministerium für Verkehr und digitale Infrastruktur: **Verordnung über die Interoperabilität des transeuropäischen Eisenbahnsystems (Transeuropäische-Eisenbahn-Interoperabilitätsverordnung)** TEIV, 2014.

[Teuber et al. 2008] Teuber, A.; Hein, G.; Kropp, V.; Paonni, M.: **Galileo Signal Fading in an Indoor Environment**. Hrsg: ION GNSS: Proceedings of the ION-GNSS 2008, Savannah, Georgia, USA, 2008.

[The London Nigerian 2011] The London Nigerian: **Eko Rail's Trains Begin Journey to Lagos**. <http://thelondonnigerian.com/2011/10/07/eko-rail%E2%80%99s-trains-begin-journey-to-lagos/>, Rev. 2011-10-07.

[Thiele 2008] Thiele, L.: **Untersuchung von Wirtschaftlichkeitsaspekten der Ortung im Schienenverkehr**. TU Braunschweig, Diplomarbeit, Braunschweig, 2008.

[Thomas et al. 2008] Thomas, M.; Lowe, D.; Dumville, M.; Roberts, W.; Cross, P.; Roberts, G.; Nunn, T.: **Dependabillity of GNSS on the UK Railways**. In: WCRR 2008. Hrsg: Korea Railroad Corporation, Korea Rail Network Authority Korea, S. 135–136: Proceedings of the 8th World Congress on Railway Research, Seoul/Korea, 2008.

[TR TS 001/2011] Eurasische Wirtschaftskommission: **Technisches Reglement "Über die Sicherheit von Schienenfahrzeugen",** Moskau, 2011. <http://www.tsouz.ru/KTS/KTS29/Pages/R_710.aspx>, Rev. 2011.

[TR TS 002/2011] Eurasische Wirtschaftskommission: **Technisches Reglement "Über die Sicherheit von Hochgeschwindigkeitseisenbahnen",** Moskau, 2011. <http://www.tsouz.ru/KTS/KTS29/Pages/R_710.aspx>, Rev. 2011.

[UIC 2013] UIC: **Railway Statistics - Synopsis 2012,** Paris, 2013. <http://www.uic.org/spip.php?article1347>.

[UNIFE 2016] UNIFE: **Information on IRIS**. <http://www.iris-rail.org/>, Rev. 2016.

[UNISIG 2012] UNISIG: **Subset 026** System Requirements Specification, Valenciennes, 2012.

[United States Congress 2008] United States Congress: **Federal Rail Safety Improvements** United States Congress, 2008.

[US Government 2012] US Government: **Official U.S. Government information about the Global Positioning System (GPS) and related topics**. <www.gps.gov>.

[US Government 2016] US Government: **Space Segment**. <http://www.gps.gov/systems/gps/space/>, Rev. 2015-12-11.

[VDV 2008] VDV: **ERTMS** Das Leitsystem für Europas Schiene. Hintergrundpapier 4/2008, Berlin, 2008.

[VDV Schrift 757] Verband Deutscher Verkehrsunternehmen VDV: **Bremsen im Betrieb bedienen und prüfen - Bremsvorschrift - BreVo -**, Flöttmann, Gütersloh, 2011, Rev. 2011.

[von Buxhoeveden/Trog 2012] von Buxhoeveden, G.; Trog, C.: **INESS: Toolunterstützung bei der Erstellung des Sicherheitsnachweises**, in: Signal+Draht, 107 (2012) 5.

[VV BAU-STE 4.6 2014] Eisenbahnbundesamt (EBA): **Verwaltungsvorschrift für die Bauaufsicht über Signal-, Telekommunikations- und Elektrotechnische Anlagen** VV BAU-STE 4.6, 2014.

[VV NTZ ÜGR Stufe 1 2013] Eisenbahnbundesamt (EBA): **Verwaltungsvorschrift für die Neue Typzulassung (NTZ) von Signal-, Telekommunikations- und Elektrotechnischen Anlagen** VV NTZ ÜGR Stufe 1, 2013.

[VV NTZ ÜGR Stufe 2 2013] Eisenbahnbundesamt (EBA): **Verwaltungsvorschrift für die Neue Typzulassung (NTZ) von Signal-, Telekommunikations- und Elektrotechnischen Anlagen** VV NTZ ÜGR Stufe 2, 2013.

[Weber 2010] Weber, C.: **Eine Risikobetrachtung zum Zugleitbetrieb** Risikoanalyse, in: Der Eisenbahningenieur, 61 (2010) 8, S. 18–23.

[Wegener 2013] Wegener, M.: **Über die metrologische Qualität der Fahrzeugortung**. TU Braunschweig, Dissertation, Braunschweig, 2013.

[Wegener et al. 2010] Wegener, M.; Hübner, M.; Schnieder, E.: **Entwicklung eines Referenzmesssystems für Ortungssysteme im Straßenverkehr unter Berücksichtigung des Qualitätsbegriffs**. In: Automatisierungssysteme, Assistenzsysteme und eingebettete Systeme für Transportmittel. Hrsg: ITS Niedersachsen e.V.: AAET 2010. Network Communications, Braunschweig, 2010.

[Wegener et al. 2011] Wegener, M.; Hübner, M.; Schnieder, E.: **Anforderungen an ein Referenzmesssystem zur Untersuchung der GPS-Messqualität** Requirements of a Reference Measurement System for the Analysis of GPS Measurement Quality, in: Technisches Messen, 78 (2011) 7-8, S. 354–363.

[Wegener/Schnieder 2013] Wegener, M.; Schnieder, E.: **Design of a mobile GNSS reference system for road vehicle localisation**. Hrsg: ITS : ITS World Congress Tokyo, Tokyo, 2013.

[Wiescholek et al. 2015a] Wiescholek, U.; Potrafke, M.; Wolters, G.; Behrends, D.; Seemann, M.; Wölfel, U.; Bantel, A.: **Die neuen Technischen Spezifikationen für die Interoperabilität**, in: Eisenbahntechnische Rundschau, 64 (2015) 6, S. 45–51.

[Wiescholek et al. 2015b] Wiescholek, U.; Potrafke, M.; Wolters, G.; Behrends, D.; Seemann, M.; Wölfel, U.; Bantel, A.: **Die neuen Technischen Spezifikationen für die Interoperabilität – Teil 2**, in: Eisenbahntechnische Rundschau, 64 (2015) 7+8, S. 14–19.

[Winter 2009] Winter, P.: **Compendium on ERTMS** European rail traffic management system, 1, Eurailpress, Hamburg, 2009.

[Wullerstorff 2010] Wullerstorff, B.v.: **InteGRail** Intelligent Integration of Railway Systems, Brüssel, 2010.

[Yarman 2015] Yarman, S.: **Latest Communication and Signalization Technologies in Railways**. In: IC-ARE'15. Hrsg: Universität Istanbul: International Congress on Advanced Railway Engineering, Istanbul, 2015.

[Yurdakul 2016] Yurdakul, A.: **Morphologisch-semantische modellierung internationaler fachsprache**, Peter Lang, Frankfurt am Main, Berlin, Bern, Bruxelles, New York, Oxford, Wien, 2016.

[Zogg 2009] Zogg, J.-M.: **GPS - Essentials of Satellite Navigation** locate, communicate, accelerate. Compendium, Thalwil, Schweiz, 2009.

[Zukunft et al. 2005] Zukunft, D.; Giszczak, A.; Meyer zu Hörste, M.; Noack, T.; Strang, T.; Lenz, B.; Schäfer, R.-P.; Schlingelhof, M.: **GALILEO im Verkehr** Anwendungspotential und DLR-Expertisen, Köln, 2005.

Abbildungsverzeichnis

Abbildung 1-1: Abgrenzung zu anderen Arbeiten und genutzte Vorarbeiten 5
Abbildung 1-2: Struktur dieser Arbeit 10
Abbildung 2-1: Zugbeeinflussungssysteme in Europa nach [Meyer zu Hörste 2004] 13
Abbildung 2-2: Migration im Schienenverkehr nach [Obrenovic 2009] 18
Abbildung 2-3: ETCS-Migration: ETCS Level 2 19
Abbildung 2-4: ETCS-Migration: ETCS Level 3- 20
Abbildung 2-5: mögliches ETCS Level 4 20
Abbildung 2-6: Gliederung von Sensoren nach [Schnieder 2007; Maschek 2015] 23
Abbildung 2-7: Ausprägungen und Komponenten eines Ortungssystems 27
Abbildung 2-8: GNSS und ihre Ausprägungen sowie Komponenten 28
Abbildung 2-9: Segmente von GNSS nach [Schnieder et al. 2009a; Poliak 2009] 29
Abbildung 2-10: Aktuelle und prognostizierte Anzahl der betriebsfähigen Satelliten im Weltall [Federal Space Agency 2016; US Government 2016; GSC 2016; China National Space Administration 2016] 31
Abbildung 2-11: SBAS und ihre Ausprägungen 33
Abbildung 3-1: Legislative und normative Dokumente in der EU – historische Entwicklung 43
Abbildung 3-2: Struktur des normativen Rahmens nach [Rüthers/Fischer 2010; Schnieder/Schnieder 2013] 46
Abbildung 3-3: Normativer Rahmen im Schienenverkehr 48
Abbildung 3-4: Übersicht der Technischen Spezifikationen für Interoperabilität mit Stand 1.1.2015 [ERA 2014; Amt für Veröffentlichungen 2014] 49
Abbildung 3-5: Struktur des Sicherheitsnachweises entsprechend des normativen Rahmens [DIN EN 50129; May 2010] 55
Abbildung 3-6: Struktur des Sicherheitsnachweises in verschiedenen Domänen [Edwards 2000; DIN EN 50129; Maguire 2006] 61
Abbildung 3-7: Elemente zur Erarbeitung des Lastenhefts [Leining et al. 2013] 65
Abbildung 3-8: Vorgeschlagene Struktur der Entwicklung und Dokumentation eines technischen Systems 70
Abbildung 4-1: Prozess der sicheren Systementwicklung 73
Abbildung 4-2: Entwicklungsprozess mit Lebenszyklus verknüpft [DIN EN 50126; DIN EN 50128] 75
Abbildung 4-3: Normativ festgelegte Organisationsstruktur nach [DIN EN 50128] 77
Abbildung 4-4: Entwicklungsprozess und Verantwortlichkeiten nach [Schnieder 2009; GAUSS Basisprojekt 2010; DIN EN 50129] 78
Abbildung 4-5: Nutzung der Abstraktionshierarchie zur Systemdarstellung nach [Schnieder/Schnieder 2010] 83

Abbildung 4-6: Übersicht der verwendeten UML-Relationen 85

Abbildung 4-7: Funktionsaspekt nach [DIN EN 15380-2; DIN EN 81346-1; DIN EN 15380-4] 87

Abbildung 4-8: Produktaspekt nach [DIN EN 15380-2; DIN EN 81346-1] 88

Abbildung 4-9: Ortsaspekt nach [DIN EN 15380-1; DIN ISO 81346-3] 89

Abbildung 4-10: Kombination des Funktions-, Produkts- und Ortsaspekts 90

Abbildung 5-1: Struktur der Darstellung der Anwendungen der satellitenbasierten Ortung im Schienenverkehr 92

Abbildung 5-2: Anwendungen der Ortung der Kategorie Verkehrsobjekt [Zukunft et al. 2005; Grimm et al. 2005; Strang 2007] 93

Abbildung 5-3: Anwendungen der Ortung der Kategorie Verkehrsleittechnik [Meyer zu Hörste 2004; Zukunft et al. 2005; Grimm et al. 2005; Strang 2007; EBA 2012] 93

Abbildung 5-4: Anwendungen der Ortung der Kategorie Verkehrsmittel [Meyer zu Hörste 2004; Zukunft et al. 2005; Grimm et al. 2005; Strang 2007; EBA 2012] 94

Abbildung 5-5: Anwendungen der Ortung der Kategorie Verkehrswegeinfrastruktur [Meyer zu Hörste 2004; Zukunft et al. 2005; Grimm et al. 2005; Strang 2007] 95

Abbildung 6-1: Zugbeeinflussungssystem mit satellitenbasierter Ortung 97

Abbildung 6-2: Analyse und Klassifikation von internen und externen Gefährdungen [Meyer zu Hörste 2004] 99

Abbildung 6-3: Generische Funktionen eines Zugbeeinflussungssystems nach [Meyer zu Hörste 2004] 100

Abbildung 6-4: Funktionsaspekt angewandt auf satellitenbasierte Ortung im Schienenverkehr 101

Abbildung 6-5: Anforderungen an Funktion der satellitenbasierten Ortung 102

Abbildung 6-6: Anforderungen einer beispielhaften Anwendung an die Ortung/ Funktion 104

Abbildung 7-1: Struktur dieses Kapitels und des betrachteten Sicherheitsnachweises. 110

Abbildung 7-2: Standardsystemarchitektur der satellitenbasierten Ortungseinheit 113

Abbildung 7-3: Fahrzeugarchitektur der satellitenbasierten Ortungseinheit entsprechend des Ortsaspekts 116

Abbildung 7-4: Fahrzeugarchitektur – strukturierte Sensorankopplung entsprechend des Orts- und Funktionsaspekts 117

Abbildung 7-5: Fahrzeugarchitektur entsprechend des Produktaspekts 118

Abbildung 7-6: Modell der Risikogenese kombiniert mit Sicherheitsimplementierung durch Vermeidung und Abwehr von Gefährdungen nach [Drewes 2009; Schnieder et al. 2009b; Schnieder 2010; Schnieder/Schnieder 2013; Müller 2015] 122

Abbildung 7-7: Generischer Prozess für sicheren Zustand in Schienenverkehr und satellitenbasierter Ortung.....129

Abbildung 7-8: Attributhierarchie der Integrität [EC/ESA 2002].....131

Abbildung 7-9: Zu zertifizierende Komponenten der satellitenbasierten Ortungseinheit.....135

Tabellenverzeichnis

Tabelle 2-1: Systemparameter (Sollwerte der realisierten und geplanten GNSS) [Bauer 2011] 30

Tabelle 2-2: IGS GPS-Produkte [Bauer 2011] 32

Tabelle 2-3: Anforderungen der Luftfahrt an GNSS [ICAO 2004] 34

Tabelle 3-1: International genutzte Normen im Schienenverkehr und ihre Verwendung 59

Tabelle 4-1: Aufgaben der Institutionen im Entwicklungsprozess nach [Maguire 2006; DIN EN 50128; VV NTZ ÜGR Stufe 2 2013] 76

Tabelle 4-2: Zuordnung von tolerierbarer Gefährdungsrate zu Sicherheitsintegritätsleveln im Schienenverkehr [DIN EN 50129] 77

Tabelle 4-3: Verantwortlichkeiten während der Zertifizierung nach [EU/2011/217; BMVBS 2013; Wiescholek et al. 2015a] 80

Tabelle 5-1: Relevante Anwendungen der satellitenbasierten Ortung im Schienenverkehr 96

Tabelle 6-1: Anforderungen an die Ortungseinheit im Schienenverkehr 103

Tabelle 7-1: Kombinatorische Verknüpfung der Systemzustände 120

Tabelle 7-2: Mögliche systematische Fehler von Systemkomponenten der satellitenbasierten Ortungseinheit 130

Tabelle 8-1: Struktur des Gutachtens für sicherheitsrelevante Systeme im Schienenverkehr 146

Tabelle 8-2: Einteilung der Abweichungen von Anforderungen im Sicherheitsnachweis 147

Tabelle 9-1: Vorteile der Nutzung der satellitenbasierten Ortung im Schienenverkehr 150